Códigos electrónicos

# Normativa para ingreso en el CSTIC (II): Temas Específicos

Selección y ordenación:
Editorial BOE. Aviso Legal: La Agencia Estatal BOE no se responsabiliza de que la normativa recopilada en este Código constituya la totalidad del contenido de los temarios, ni garantiza los cambios que pueda realizar el órgano convocante

Edición actualizada a 6 de agosto de 2024

**BOLETÍN OFICIAL DEL ESTADO**

**INAP**

La última versión de este Código en PDF y ePUB está disponible para su descarga **gratuita** en:
www.boe.es/biblioteca_juridica/

Alertas de actualización en Mi BOE: www.boe.es/mi_boe/

Para adquirir el Código en formato papel: tienda.boe.es


NIPO (PDF): 090-22-095-8
NIPO (Papel): 090-22-094-2
NIPO (ePUB): 090-22-096-3
ISBN: 978-84-340-2819-7
Depósito Legal: M-11695-2022

Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

Agencia Estatal Boletín Oficial del Estado
Avenida de Manoteras, 54
28050 MADRID
www.boe.es

# SUMARIO

## SUMARIO

## SUMARIO

## II. TECNOLOGÍA BÁSICA

## III. INGENIERÍA DE LOS SISTEMAS DE INFORMACIÓN

## IV. REDES, COMUNICACIONES E INTERNET

# ÍNDICE SISTEMÁTICO

II. TECNOLOGÍA BÁSICA

III. INGENIERÍA DE LOS SISTEMAS DE INFORMACIÓN

IV. REDES, COMUNICACIONES E INTERNET

# § 1

## INTRODUCCIÓN

El Código electrónico sobre la "Normativa para ingreso en el Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado: Temas Específicos (II)", ha sido elaborado por la Editorial del Boletín Oficial del Estado como ayuda al opositor para la preparación del programa exigido en la última convocatoria al Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado publicada en el BOE del 8 de junio de 2023 (Resolución de 6 de junio de 2023, de la Secretaría de Estado de Función Pública, por la que se convoca el proceso selectivo para ingreso, por el sistema general de acceso libre y promoción interna, en el Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado).

Dado el gran volumen de normativa jurídica que habría que consultar para poder abarcar todo el programa de la oposición y, para dar mayor facilidad de consulta a los opositores y/o ciudadanos interesados, se ha optado por dividir esta obra de compilación en 2 volúmenes: temas generales y temas específicos.

El Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado (TIC) está clasificado en el Subgrupo A1, por lo que para poder presentarse a las pruebas selectivas de acceso al mismo se exige estar en posesión del título universitario de Grado, Licenciatura, Ingeniería o Arquitectura.

Se crea con carácter de cuerpo general interministerial en el año 1990, estando adscrito actualmente al Ministerio de Hacienda y Función Pública.

Las funciones desempeñadas por los miembros del Cuerpo Superior de Sistemas y Tecnologías de la Información de la Administración del Estado (TIC) se desarrollan habitualmente en el entorno de las tecnologías de la información y las telecomunicaciones. Sus miembros asumen responsabilidades en la dirección de las unidades administrativas relacionadas con estas áreas tecnológicas, así como en la dirección de proyectos informáticos y de telecomunicaciones en órganos centrales y territoriales de los Ministerios, Organismos Públicos de la Administración General del Estado y de la Seguridad Social, así como en la Administración en el exterior.

El valor añadido de esta compilación legislativa reside en la constante actualización por parte de la Agencia Estatal Boletín Oficial del Estado (AEBOE) de las normas jurídicas de su base de datos consolidada, lo que permite al lector confiar en la plena validez de los textos compilados.

La utilidad de acceder a una fuente consolidada y permanentemente actualizada como las bases de datos que ofrece la AEBOE, resulta incuestionable; dado que es un instrumento útil para conocer la legislación estatal de aplicación general, reforzando la seguridad jurídica y la transparencia del sector normativo, permitiendo acceder a la información de una forma más eficiente y económica (descargas gratuitas en formatos electrónicos PDF y ePUB) y teniendo una capacidad de búsqueda más avanzada mediante los hipervínculos que proporcionan el acceso directo al precepto buscado, contribuyendo así al objetivo de conseguir una Administración más abierta y cercana al ciudadano.

De esta manera, la ciudadanía, los opositores, estudiantes o profesionales en el ejercicio de su actividad, tienen una potente y fiable herramienta informativa que les permite saber en cada momento qué normas están vigentes para aquellos asuntos que puedan ser de su interés.

En el sumario de este segundo volumen, dedicado al grupo de temas específicos, se ofrece al lector una selección de las normas más destacadas del programa -a texto completo-; asimismo, el resto de las disposiciones que va a complementar este grupo de materias técnicas podrán ser igualmente consultadas -a texto completo- mediante los enlaces web (link) a la base de datos consolidada de la AEBOE o a cada uno de los códigos que se relacionan a continuación y que amplian la materia de estudio.

**OTRAS FUENTES DE CONSULTA (Códigos Electrónicos del BOE):**

**Derecho Constitucional**

**Código de Derecho Constitucional**

**Derecho Administrativo General**

**Código de Derecho Administrativo**

**Procedimiento Administrativo Común**

**Código de Administración Electrónica**

**Código de Contratos del Sector Público**

**Organización Administrativa**

**Código de la estructura de la Administración General del Estado**

**Estatutos de Autonomía**

**Código de la estructura de la Administración Institucional del Estado**

**Código de Régimen Local**

**Función Pública**

**Código de la Función Pública**

**Seguridad Vial, Transporte y Telecomunicaciones**

**Código de las Telecomunicaciones**

**Código de Derecho Audiovisual**

**Nota importante**:

Los textos consolidados que la Agencia Estatal BOE ofrece tienen carácter meramente **informativo** y carecen de validez jurídica alguna. Para fines jurídicos deben utilizarse los textos publicados en el diario "Boletín Oficial del Estado".

Todas las versiones consolidadas tienen Permalink ELI: se trata de un enlace permanente a las distintas versiones del texto consolidado, que pretende facilitar su búsqueda y localización en internet. Este enlace se construye de acuerdo con el estándar europeo ELI (Identificador Europeo de Legislación).

# § 2

## Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos

Ministerio de la Presidencia
«BOE» núm. 234, de 26 de septiembre de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-9741

Durante los últimos años hemos asistido a profundos cambios en la Administración en relación a la utilización de las tecnologías de la información y las comunicaciones (TIC). Cambios caracterizados, en una primera fase, por el uso de estas tecnologías en la automatización y mejora del funcionamiento de los procesos internos de la Administración, en el convencimiento de que el ahorro derivado de la mejora de la eficiencia se trasladaría a los ciudadanos. Posteriormente, por la universalización de Internet y de las tecnologías asociadas que ha propiciado el desarrollo de nuevos servicios y formas de relación con los ciudadanos y empresarios en un camino sin retorno hacia la Administración electrónica.

La confluencia de nuevas tendencias tecnológicas como son los llamados servicios en la nube (cloud computing), la aparición de dispositivos móviles cada vez más inteligentes, la generalización del uso de las redes sociales, la capacidad de análisis de grandes volúmenes de datos (big data) junto con la universalización del uso de Internet, han conformado un nuevo panorama en el que los ciudadanos han adquirido nuevos hábitos y expectativas en la utilización de los servicios digitales en su ocio, en su relación con las empresas y también con las Administraciones Públicas.

La digitalización de los servicios engloba, por una parte, a los servicios electrónicos y a las tecnologías de la información y las comunicaciones, que han sido la base de la Administración electrónica en la que España ha alcanzado un avance reseñable.

Pero la digitalización supone también afrontar nuevos retos y oportunidades. La confluencia de estas nuevas fuerzas tecnológicas lleva a un nuevo panorama en el que la Administración debe ser capaz de adaptarse de manera ágil a nuevas demandas de un entorno cambiante, proporcionar información y servicios digitales en cualquier momento, en cualquier lugar y por diferentes canales, generar nuevas formas de relación con los ciudadanos e innovar nuevos servicios, aprovechando las oportunidades que proporcionan estas tecnologías. Y todo ello debe ser provisto de manera segura, ágil y con eficacia y eficiencia en la utilización de los recursos disponibles.

No se trata por lo tanto de la utilización de las TIC en los procesos de la Administración, sino de crear las dinámicas necesarias para poder adaptar los servicios, procesos, operaciones y las capacidades de la Administración a una realidad que es digital y seguirá evolucionando previsiblemente a gran velocidad.

La Administración debe adoptar una nueva cultura de la información y estar preparada para recoger, generar y tratar grandes volúmenes de información digital sobre sus operaciones, procesos y resultados, que podrá ser puesta convenientemente a disposición de ciudadanos para el impulso de la transparencia, y de empresas y agentes sociales para el fomento de la reutilización de la información del sector público. Asimismo, el desarrollo de las capacidades de análisis transversal de la información permitirá optimizar la gestión, mejorar la toma de decisiones y ofrecer servicios interdepartamentales de manera independiente a la estructura administrativa.

Por otra parte, la universalización de los servicios digitales y las nuevas formas de relación con los ciudadanos permiten conformar una Administración más transparente, en la que los ciudadanos puedan participar en la definición e incluso en el diseño de los servicios públicos, de forma que estos se adapten mejor a las necesidades reales de los ciudadanos en un nuevo modelo de gobernanza.

Todo este entorno supone un nuevo mundo de oportunidades, pero también de amenazas, que deben ser afrontados desde un inicio generando en la Administración las sinergias necesarias para aprovechar el talento de las personas que conforman aquélla, sumando los esfuerzos y recursos disponibles y diseñando una estrategia común para la transformación digital de la Administración, basada en las TIC y orientada a la generación de valor para los ciudadanos.

El informe elaborado por la Comisión para la Reforma de las Administraciones Públicas (CORA), creada por Acuerdo de Consejo de Ministros de 26 de octubre de 2012, y presentado al Consejo de Ministros de 21 de junio de 2013, reconoce este papel fundamental de las TIC y aconseja un tratamiento singular respecto a otros servicios comunes a fin de obtener el máximo de eficacia y de optimización de recursos y aprovechar las oportunidades que supone la actuación coordinada de acuerdo a una estrategia común.

El reconocimiento del papel de las tecnologías de la información y las comunicaciones en la transformación de la Administración estaba ya recogido, entre otras, pero muy especialmente, en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que partía del reconocimiento del insuficiente desarrollo de la administración electrónica, y consideraba que la causa en buena medida se debía a que las previsiones de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común tienen carácter facultativo. Es decir, que dejan en manos de las propias Administraciones determinar si los ciudadanos van a poder de modo efectivo, o no, relacionarse por medios electrónicos con ellas, según que éstas quieran poner en pie los instrumentos necesarios para esa comunicación con la Administración. Por ello esa ley pretendió dar el paso del «podrán» por el «deberán».

La Ley 11/2007, de 22 de junio, consagra la relación con las Administraciones Públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para tales Administraciones.

El contexto europeo, la Agenda Digital para Europa, propone también medidas legales para el efectivo desarrollo digital de la Unión Europea. El impulso de una administración digital supone también, por tanto, dar respuesta a los compromisos comunitarios estableciendo así un marco operativo y jurídicamente claro con el fin de eliminar la fragmentación y la ausencia de interoperabilidad, potenciar la ciudadanía digital y prevenir la ciberdelincuencia.

Un buen uso de las TIC, eficiente e integrado, resulta también imprescindible para cumplir con los compromisos que la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno establecen para la Administración.

A esta voluntad de constituir las TIC como herramienta de vertebración de la mejora del funcionamiento de las administraciones responde la creación de la Dirección de Tecnologías de la Información y las Comunicaciones de la Administración General del Estado, por Real Decreto 695/2013, de 20 de septiembre. La Dirección se configura, de acuerdo con su norma de creación, como un órgano específico, al más alto nivel, para impulsar y coordinar el necesario proceso de racionalización y transformación de las diversas facetas de la política de tecnologías de la información y de las comunicaciones en todo el ámbito del Sector Público Administrativo Estatal. En virtud del Real Decreto 802/2014, de 19 de septiembre, dicho órgano se adscribe al Ministerio de Hacienda y Administraciones Públicas.

El proceso de transformación que se encomienda a la Dirección de Tecnologías de la Información y las Comunicaciones supone revisar planteamientos organizativos vigentes, algunos de los cuales se ponen de manifiesto en el propio informe CORA, entre ellos, la existencia de un elevado grado de atomización y un alto nivel de independencia en la actuación de los agentes que intervienen en el ámbito de las TIC en la Administración General del Estado y sus Organismos Públicos.

Esta situación propicia una elevada autonomía en la gestión de los fondos y recursos TIC por parte de los diferentes órganos de la Administración Pública, siendo en cada una de ellos donde se toman las decisiones de gastos e inversión, lo que ha dado lugar a una dispersión considerable de recursos y esfuerzos en materia TIC, si bien las Subsecretarías y demás órganos competentes en materia de tecnologías de la información y las comunicaciones, a través de las unidades TIC de la Administración General del Estado y sus Organismos Públicos han sido capaces de atender una demanda creciente de servicios y unas exigencias elevadas, que han situado la oferta actual de servicios en niveles equivalentes o superiores a la media de la Unión Europea.

El modelo de gobernanza sobre el que se asienta este real decreto pretende superar esa situación, con el fin de conseguir una política TIC común a toda la Administración General del Estado y sus Organismos Públicos en un contexto de austeridad en el gasto público basado en la exigencia de eficiencia y corresponsabilidad. La Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, tiene uno de sus pilares en los principios de eficiencia en la asignación y utilización de los recursos públicos. Siguiendo el mandato de esta ley, este real decreto contiene disposiciones en materia de planificación de la acción TIC con implicaciones normativas, organizativas, presupuestarias y contractuales que se encuadran en un marco de planificación plurianual, y de programación y presupuestación, que ha de atender a la situación económica, a los objetivos de política económica y al cumplimiento de los principios de estabilidad presupuestaria y sostenibilidad financiera. En desarrollo de lo que dispone la Ley Orgánica 2/2012, de 27 de abril, este real decreto crea instrumentos para contribuir a una gestión de los recursos públicos orientada a la eficacia, la eficiencia, la economía y la calidad, instrumentos imprescindibles para la aplicación de políticas de racionalización del gasto y de mejora de la gestión del sector público.

La estructura de gobernanza de las TIC en la Administración General del Estado y sus Organismos Públicos ha tenido hasta la fecha sus pilares en los órganos colegiados de Administración electrónica. Por una parte, el Consejo Superior de Administración Electrónica, órgano máximo en materia de Administración electrónica del que han emanado las principales líneas y proyectos de Administración electrónica de la Administración General del Estado. Por otra parte, adscritas a los diferentes departamentos Ministeriales, las Comisiones Ministeriales de Administración electrónica (CMAEs).

Las CMAEs han permitido realizar el seguimiento y control de las diferentes inversiones y gastos TIC en el ámbito Ministerial pero, debido a la propia atomización de las unidades ministeriales, no ha sido posible desarrollar, salvo en algunos Ministerios, la labor de diseñar, junto a las unidades administrativas ministeriales, la estrategia digital que soporte los procesos administrativos sectoriales competencia de cada departamento.

En este sentido, la digitalización de la Administración supone no sólo la transformación de los servicios ofrecidos a medios electrónicos, utilizando para ello las capacidades que ofrecen las TIC, sino que apuesta por el rediseño integral de los procesos y servicios actuales de la Administración, permitiendo nuevos modelos de relación con los ciudadanos y habilitando la prestación de servicios innovadores que no serían realizables sin un necesario cambio cultural.

Es fundamental, por lo tanto, contar con unidades TIC ministeriales, que conozcan profundamente el ámbito de trabajo específico del departamento para diseñar servicios digitales adaptados a las necesidades de ciudadanos y empresas, aprovechando la gran capacitación y el conocimiento especializado del personal TIC para el desarrollo y operación de las aplicaciones sectoriales específicas de cada unidad de negocio. Su principal objetivo será impulsar el proceso de transformación digital de la Administración General del Estado y sus Organismos Públicos, que ha de tener por fin no sólo la automatización de los servicios, sino su rediseño integral, aprovechando las capacidades que permiten las nuevas

tecnologías con el fin de implantar nuevos y mejores modelos de relación con los ciudadanos, con servicios más eficientes que faciliten el crecimiento económico.

En este sentido, las Comisiones Ministeriales actuales deben evolucionar su papel hacia la elaboración del proyecto del plan de acción sectorial del departamento en materia de Administración digital, atendiendo de forma priorizada las propuestas y necesidades de los distintos órganos y organismos públicos afectados y promoviendo la compartición de los servicios. De esta manera, las actuales unidades ministeriales de tecnologías de la información y de las comunicaciones se convertirán en las unidades responsables del soporte y la transformación digital de los diferentes ámbitos departamentales.

Los motivos expuestos anteriormente llevan a la necesidad de rediseñar el modelo de gobernanza de las TIC en la Administración General del Estado y sus Organismos Públicos. El desarrollo de este nuevo modelo se ha encomendado a un órgano de nueva creación, específico y al máximo nivel, la Dirección de Tecnologías de la Información y las Comunicaciones de la Administración General del Estado.

Para el diseño de la nueva gobernanza TIC, desde la Dirección de Tecnologías de la Información y las Comunicaciones se han identificado tres objetivos básicos:

Primero, orientar las actuaciones y líneas estratégicas en las TIC de forma que tengan como principal objetivo satisfacer las necesidades derivadas de la estrategia global del Gobierno y disponer de una planificación estratégica común para toda la Administración General del Estado y sus Organismos Públicos.

Segundo, potenciar la Administración digital y las TIC como los instrumentos que permitan hacer sostenible el constante proceso de innovación y mejora en la calidad de los servicios ofrecidos por la administración que demandan ciudadanos y empresas, e incrementar la productividad de los empleados públicos.

Tercero, racionalizar el uso de los recursos informáticos de forma que se consiga una mayor eficiencia, proporcionando un ahorro sustancial de costes de todo tipo, y en especial en el resto de la actividad administrativa, como consecuencia de una mayor homogeneidad y simplicidad mediante el uso de herramientas comunes y servicios compartidos, objetivo de especial interés en un contexto de limitación presupuestaria.

En todo caso, se hace necesario favorecer el diseño de sistemas de compras que sean capaces de conseguir ahorros importantes, adoleciendo el proceso de contratación actual de falta de flexibilidad para aprovechar el estado de madurez del sector TIC español. Esta dispersión de las contrataciones TIC en diferentes unidades ha derivado en una gran diversidad de suministradores en la contratación de productos y servicios idénticos, lo que impacta en mayores costes de mantenimiento y evolución, por lo que es necesario racionalizar el proceso de contratación y dotarlo de mecanismos ágiles que favorezcan el aprovechamiento de economías de escala como consecuencia de la agregación de la demanda. En este sentido, la Dirección de Tecnologías de la Información y las Comunicaciones propondrá a la Dirección General de Racionalización y Centralización de la Contratación los contratos de suministros, obras y servicios en materia TIC que deban ser declarados de contratación centralizada por el titular del Ministerio de Hacienda y Administraciones Públicas.

Asimismo, la Dirección de Tecnologías de la Información y las Comunicaciones, se encargará de alinear las inversiones TIC con los objetivos estratégicos establecidos.

El nuevo modelo de gobernanza TIC persigue centralizar las competencias y los medios para desempeñarlas en un único órgano administrativo en el que se integren todas las unidades TIC de la Administración General del Estado y sus Organismos Públicos, articulándose su interacción con el resto de áreas de la Administración, a las que prestan sus servicios, mediante unos nuevos órganos colegiados que sirvan como canal ágil de información y puesta en común de necesidades y oportunidades de utilización de medios informáticos de forma racional y eficiente.

Ello supondrá, por tanto, la capacitación para la prestación de servicios compartidos TIC a todas las unidades de la Administración General del Estado y sus Organismos Públicos y la definición de una estrategia común que definirá las líneas de actuación en materia TIC de los órganos y organismos de la Administración General del Estado y sus Organismos Públicos.

A tales efectos, se crean la Comisión de Estrategia TIC y, en el ámbito departamental, las Comisiones Ministeriales de Administración Digital como órganos colegiados encargados de impulsar la transformación digital de la Administración de acuerdo a una Estrategia común en el ámbito de las Tecnologías de la Información y las Comunicaciones. Asimismo, este real decreto deroga el Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados responsables de la Administración electrónica, quedando suprimidos el Consejo Superior de Administración Electrónica y las Comisiones Ministeriales de Administración Electrónica. Este nuevo modelo de Gobernanza en el ámbito de las Tecnologías de la Información y las Comunicaciones se alcanzará de manera paulatina en un proceso que, partiendo desde la heterogeneidad y dispersión actual converja hacia un modelo de prestación de servicios compartidos e infraestructuras comunes de forma que pueda garantizarse el mantenimiento del nivel de servicio actual y la paulatina implementación de sinergias e incremento de eficiencia, simplificación de estructuras y, por tanto, mejora de la productividad de la Administración.

Para hacer efectivas estas medidas, este real decreto no sólo se aplica a la Administración General del Estado, sus organismos autónomos y entidades gestoras y servicios comunes de la Seguridad Social, sino que se prevé su aplicación a otras entidades públicas, cuya actuación pueda presentar una especial trascendencia en la prestación de servicios públicos electrónicos y en el propio desarrollo de la Administración digital.

En su virtud, a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia, y del Ministro de Hacienda y Administraciones Públicas, y previa deliberación del Consejo de Ministros en su reunión del día 19 de septiembre de 2014,

DISPONGO:

## CAPÍTULO I

## Objeto y ámbito de aplicación

**Artículo 1.** *Objeto.*

El objeto de este real decreto es el desarrollo y ejecución de un modelo común de gobernanza de las Tecnologías de la Información y las Comunicaciones (TIC) en la Administración General del Estado y sus Organismos Públicos.

Este modelo de Gobernanza de las TIC incluirá, en todo caso, la definición e implementación de una estrategia global de transformación digital que garantice el uso adecuado de los recursos informáticos de acuerdo a las necesidades derivadas de la estrategia general del Gobierno, con el fin de mejorar la prestación de los servicios públicos al ciudadano.

**Artículo 2.** *Ámbito de aplicación.*

El ámbito de aplicación de este real decreto se extiende a la Administración General del Estado y sus Organismos Públicos previstos en el artículo 43 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

## CAPÍTULO II

## Órganos con competencias en materia de Administración digital

**Artículo 3.** *La Comisión de Estrategia TIC. Objeto, adscripción y funcionamiento.*

1. La Comisión de Estrategia TIC es el órgano colegiado encargado de la definición y supervisión de la aplicación de la Estrategia sobre Tecnologías de la Información y las Comunicaciones de la Administración General del Estado y sus organismos públicos, «Estrategia TIC», que será aprobada por el Gobierno de acuerdo con lo previsto en el artículo 9 de este Real Decreto.

2. La Comisión de Estrategia TIC se adscribe al Ministerio de Hacienda y Administraciones Públicas a través de la Secretaría de Estado de Administraciones Públicas.

3. La Comisión de Estrategia TIC actuará en pleno y por medio de su comité ejecutivo.

**Artículo 4.** *Funciones de la Comisión de Estrategia TIC.*

1. Corresponde a la Comisión de Estrategia TIC el ejercicio de las siguientes funciones:

a) Fijar las líneas estratégicas, de acuerdo con la política establecida por el Gobierno, en materia de tecnologías de la información y las comunicaciones, para el impulso de la Administración digital en la Administración General del Estado y sus organismos públicos.

b) Aprobar la propuesta de Estrategia TIC de la Administración General del Estado y sus organismos públicos para su elevación al Consejo de Ministros por los titulares de los departamentos de Hacienda y Administraciones Públicas y de la Presidencia.

c) Informar los anteproyectos de ley, los proyectos de disposiciones reglamentarias y otras normas de ámbito general que le sean sometidos por los órganos proponentes cuyo objeto sea la regulación en materia TIC de aplicación en la Administración General del Estado y sus Organismos Públicos o de los recursos de carácter material y humano afectos a su desarrollo.

d) Definir las prioridades de inversión en materias TIC de acuerdo con los objetivos establecidos por el Gobierno.

e) Declarar los medios o servicios compartidos en los términos establecidos en el artículo 10.

f) Declarar los proyectos de interés prioritario, en los términos establecidos en el artículo 11, a propuesta de los ministerios y sus organismos públicos adscritos previo informe de la Dirección de Tecnologías de la Información y las Comunicaciones. Se considerarán proyectos de interés prioritario aquellos que por sus especiales características sean fundamentales para la mejora de la prestación de servicios al ciudadano.

g) Impulsar la colaboración y cooperación con las comunidades autónomas y las entidades locales para la puesta en marcha de servicios interadministrativos integrados y la compartición de infraestructuras técnicas y los servicios comunes que permitan la racionalización de los recursos TIC a todos los niveles del Estado.

h) Impulsar las actividades de cooperación de la Administración General del Estado y sus Organismos Públicos con la Unión Europea, con las organizaciones internacionales y, especialmente, con Iberoamérica, en materia de tecnologías de la información y Administración digital, en colaboración con el Ministerio de Asuntos Exteriores y de Cooperación.

i) Actuar como Observatorio de la Administración Electrónica y Transformación Digital.

2. La Comisión de Estrategia TIC elevará anualmente, a través de su Presidente, un informe al Consejo de Ministros, en el que se recogerá el estado de la transformación digital de la Administración en la Administración General del Estado y sus organismos públicos.

**Artículo 5.** *Composición y funcionamiento del Pleno de la Comisión de Estrategia TIC.*

1. El Pleno de la Comisión de Estrategia TIC estará integrado por los titulares de las Secretarías de Estado de Administraciones Públicas, de Telecomunicaciones y para la Sociedad de la Información y de Seguridad Social, así como por los Subsecretarios o, bien, el titular de un órgano superior de los distintos Departamentos ministeriales y el Director de Tecnologías de la Información y las Comunicaciones. Será presidido por el Ministro de Hacienda y Administraciones Públicas y actuará como Secretario el Director de Tecnologías de la Información y las Comunicaciones.

2. Las reuniones del Pleno se celebrarán, al menos, dos veces al año por convocatoria de su Presidente, bien a iniciativa propia, bien cuando lo soliciten, al menos, la mitad de sus miembros.

3. El Presidente podrá invitar a incorporarse, con voz pero sin voto, a representantes de otras instituciones públicas o privadas.

4. Las funciones de asistencia y apoyo a la Comisión de Estrategia TIC y a su Comité Ejecutivo serán desempeñadas por la Dirección de Tecnologías de la Información y las Comunicaciones.

5. Por acuerdo de la Comisión de Estrategia TIC se podrán constituir los grupos de trabajo que se requieran para el adecuado desarrollo de sus funciones.

**Artículo 6.** *Composición y funcionamiento del Comité Ejecutivo de la Comisión de Estrategia TIC.*

1. El Comité Ejecutivo de la Comisión de Estrategia TIC se constituye como el instrumento de la Comisión de Estrategia TIC para asegurar una actuación ágil y efectiva de la Estrategia TIC en la Administración General del Estado y sus Organismos Públicos.

2. El Comité Ejecutivo de la Comisión de Estrategia TIC estará presidido por el Director de Tecnologías de la Información y las Comunicaciones, estará compuesto por un mínimo de cinco miembros, un máximo de diez miembros y su composición será determinada por la Comisión de Estrategia TIC.

Actuará como secretario un funcionario de la Dirección de Tecnologías de la Información y las Comunicaciones, que será designado por el Presidente del Comité.

3. El Comité Ejecutivo ejercerá las competencias que le atribuya expresamente el Pleno de la Comisión de Estrategia TIC, y deberá informar periódicamente a éste acerca de las decisiones y actuaciones adoptadas. En todo caso, le corresponde la aprobación de los Planes de Acción Departamentales regulados en el artículo 14 del presente real decreto.

4. Las reuniones del Comité Ejecutivo se celebrarán mensualmente. El Presidente podrá convocar al Comité con carácter extraordinario cuando resulte necesario.

5. El Presidente del Comité Ejecutivo podrá invitar a incorporarse, con voz pero sin voto, a los Presidentes de las Comisiones Ministeriales de Administración Digital cuando lo estime conveniente.

6. Podrán constituirse los grupos de trabajo que se requieran para el adecuado desarrollo de sus funciones.

**Artículo 7.** *Las Comisiones Ministeriales de Administración Digital.*

1. Las Comisiones Ministeriales de Administración Digital (CMAD) son órganos colegiados de ámbito departamental responsables del impulso y de la coordinación interna en cada departamento en materia de Administración digital, y serán los órganos de enlace con la Dirección de Tecnologías de la Información y las Comunicaciones.

Las CMAD estudiarán y planificarán las necesidades funcionales de las distintas áreas administrativas del ministerio, valorarán las posibles vías de actuación, priorizándolas, y propondrán su desarrollo, todo ello evitando que se generen duplicidades, conforme al principio de racionalización, y promoviendo la compartición de infraestructuras y servicios comunes.

El ámbito de actuación de las CMAD comprende todos los órganos del departamento y a los organismos públicos adscritos al mismo.

2. Las CMAD estarán presididas por el Subsecretario y estarán integradas por los representantes, con rango mínimo de Subdirector General, de las áreas funcionales y de los organismos adscritos que se determine mediante orden ministerial, así como los responsables de las unidades ministeriales de tecnologías de la información y las comunicaciones.

El Presidente de la CMAD podrá delegar esta función en el titular de una unidad del mismo departamento, con rango mínimo de Director General.

Podrán asistir a las reuniones de la CMAD expertos de la Dirección de Tecnologías de la Información y las Comunicaciones, que tendrán carácter de asesores, con voz y sin voto.

3. Las CMAD desempeñarán las siguientes funciones:

a) Actuar como órgano de relación entre los departamentos ministeriales y sus organismos adscritos y la Dirección de Tecnologías de la Información y las Comunicaciones, para asegurar la coordinación con los criterios y políticas definidas por ésta.

b) Impulsar, ejecutar y supervisar, en el ámbito del departamento, el cumplimiento de las directrices y el seguimiento de las pautas de actuación recogidas en la Estrategia TIC de la Administración General del Estado y sus Organismos Públicos aprobada por el Gobierno a propuesta del Comité de Estrategia TIC.

c) Elaborar el Plan de acción del departamento para la transformación digital, en desarrollo de los criterios establecidos por la Dirección de Tecnologías de la Información y las Comunicaciones atendiendo a la Estrategia TIC de la Administración General del Estado y sus Organismos Públicos, aprobada por el Consejo de Ministros.

d) Analizar las necesidades funcionales de las unidades de gestión del departamento y sus organismos adscritos y evaluar las distintas alternativas de solución propuestas por las unidades TIC, identificando las oportunidades de mejora de eficiencia que pueden aportar las TIC, aplicando soluciones ya desarrolladas en el ámbito del Sector Público y estimando costes en recursos humanos y materiales que los desarrollos TIC asociados puedan suponer

e) Impulsar la digitalización de los servicios y procedimientos del departamento con el fin de homogeneizarlos, simplificarlos, mejorar su calidad y facilidad de uso, así como las prestaciones ofrecidas a los ciudadanos y empresas, optimizando la utilización de los recursos TIC disponibles.

f) Colaborar con la Dirección de Tecnologías de la Información y las Comunicaciones en la identificación y la puesta a disposición común de los medios humanos, materiales y económicos que estén adscritos al departamento y que deban ser utilizados para la puesta en funcionamiento o mantenimiento de los medios o servicios compartidos.

g) Cualesquiera otras que determinen sus respectivas órdenes ministeriales reguladoras, de acuerdo con las peculiares necesidades de cada departamento ministerial.

4. Las CMAD analizarán los proyectos de disposiciones de carácter general de su departamento y elaborarán un informe en el que se expondrán y valorarán la oportunidad de la medida, los costes, necesidad de disponibilidad de recursos humanos y tiempos de desarrollo que se puedan derivar de la aprobación del proyecto desde la perspectiva de la utilización de medios y servicios TIC y lo remitirán a la Dirección de Tecnologías de la Información y las Comunicaciones para su conocimiento y valoración.

5. En el ejercicio de sus funciones y en su ámbito de actuación ministerial, las CMAD, formularán propuestas de aplicación de nuevos criterios de organización o de funcionamiento, implantación de nuevos procedimientos o de revisión de los existentes.

**Artículo 8.** *El Comité de Dirección de las Tecnologías de Información y Comunicaciones.*

El Comité de Dirección de las Tecnologías de Información y las Comunicaciones es un órgano de apoyo adscrito a la Dirección de Tecnologías de la Información y las Comunicaciones.

Estará integrado por el responsable TIC de las subsecretarías del órgano superior al que corresponda la coordinación de las TIC en cada uno de los departamentos ministeriales así como por los responsables de aquellas unidades TIC que por su relevancia sean designados por el Director de Tecnologías de la Información y las Comunicaciones, quién lo presidirá.

Actuará como órgano de coordinación y colaboración entre la Dirección de Tecnologías de la Información y las Comunicaciones y los órganos y organismos integrantes de la Administración General del Estado y sus Organismos Públicos a fin de establecer una acción coordinada, de acuerdo con las líneas estratégicas definidas por la Comisión de Estrategia TIC y contribuirá a definir metodologías, procesos, arquitecturas, normas y buenas prácticas comunes a todas las unidades TIC de la Administración General del Estado y sus Organismos Públicos velando por el cumplimiento de programas y proyectos, la consecución de los objetivos marcados y la eliminación de redundancias.

## CAPÍTULO III

## Modelo de gobernanza en el ámbito de las tecnologías de la información y las comunicaciones

**Artículo 9.** *Estrategia en materia de tecnologías de la información y las comunicaciones.*

El Gobierno, a iniciativa de la Comisión de Estrategia TIC, y a propuesta de los Ministros de la Presidencia, de Hacienda y Administraciones Públicas y de Industria, Energía y Turismo, aprobará la Estrategia en materia de tecnologías de la información y las comunicaciones (en adelante Estrategia TIC), así como las revisiones de la misma.

La Estrategia TIC determinará los objetivos, principios y acciones para el desarrollo de la administración digital y la transformación digital de la Administración General del Estado y sus Organismos Públicos y servirá de base para la elaboración por los distintos ministerios de sus planes de acción para la transformación digital.

La Comisión de Estrategia TIC determinará el ámbito temporal de la Estrategia TIC, así como su periodo de revisión.

**Artículo 10.** *Medios y servicios compartidos.*

1. Los medios y servicios TIC de la Administración General del Estado y sus Organismos Públicos serán declarados de uso compartido cuando, en razón de su naturaleza o del interés común, respondan a necesidades transversales de un número significativo de unidades administrativas.

A los efectos de este real decreto, se entenderá por «medios y servicios» todas las actividades, infraestructuras técnicas, instalaciones, aplicaciones, equipos, inmuebles, redes, ficheros electrónicos, licencias y demás activos que dan soporte a los sistemas de información.

Los activos TIC afectos a la prestación de servicios sectoriales se podrán mantener en sus ámbitos específicos en razón de la singularidad competencial y funcional que atienden y no tendrán, por tanto, la consideración de medios y servicios compartidos. La responsabilidad sobre la gestión de estos medios corresponderá a los departamentos ministeriales y organismos adscritos desarrollada a través de las respectivas unidades TIC con el apoyo y supervisión de la Dirección de Tecnologías de la Información y las Comunicaciones.

2. La declaración de medios y servicios compartidos necesarios para la ejecución y desarrollo de la Estrategia TIC aprobada por el Gobierno, corresponderá a la Comisión de Estrategia TIC a propuesta de la Dirección de Tecnologías de la Información y las Comunicaciones.

Cuando concurran razones económicas, técnicas o de oportunidad sobrevenidas, la Comisión de Estrategia TIC podrá autorizar al Director de Tecnologías de la Información y las Comunicaciones a acordar excepciones a la declaración de medio o servicio de uso compartido, de las que se dará traslado a los miembros de la Comisión de Estrategia TIC.

La declaración de medio o servicio compartido habilitará a la Dirección de Tecnologías de la Información y las Comunicaciones para adoptar las medidas necesarias para su provisión compartida, bien directamente o a través de otras unidades TIC y, en su caso, para disponer tanto de los medios humanos y económicos como de las infraestructuras y resto de activos TIC que los ministerios y unidades dependientes venían dedicando a atender dichos servicios, entre los que se incluyen también ficheros electrónicos y licencias.

Dada la naturaleza funcional específica y régimen competencial singular de los servicios de Informática presupuestaria de la Intervención General de la Administración del Estado, lo establecido en este apartado 2 respecto a los servicios, recursos e infraestructuras TIC comunes y al catálogo de servicios TIC comunes, cuando pueda afectar a los sistemas de funcionalidad específica de Informática presupuestaria requerirá la previa aprobación de la Intervención General de la Administración del Estado.

3. La utilización de los medios y servicios compartidos será de carácter obligatorio y sustitutivo respecto a los medios y servicios particulares empleados por las distintas unidades.

La Dirección de Tecnologías de la Información y las Comunicaciones establecerá un Catálogo de Servicios Comunes del que formarán parte los medios y servicios compartidos, así como aquellas infraestructuras técnicas o aplicaciones desarrolladas por la Dirección de Tecnologías de la Información y las Comunicaciones cuya provisión de manera compartida facilite la aplicación de economías de escala y contribuya a la racionalización y simplificación de la actuación administrativa.

4. Dentro de este Catálogo figurarán servicios de administración digital orientados a integrar todas las relaciones de las Administraciones públicas con el ciudadano, mediante la provisión compartida, que le permita tener una visión integral de sus relaciones con las Administraciones públicas y acceso a todos los servicios on-line.

5. La provisión, explotación y gestión de los medios y servicios compartidos será realizada por la Dirección de Tecnologías de la Información y las Comunicaciones, salvo los que correspondan a los servicios de informática presupuestaria de la Intervención General de la Administración del Estado. Las eficiencias que se produzcan en estos procesos se dedicarán preferentemente a potenciar los servicios sectoriales.

6. Las CMAD y las unidades TIC sectoriales velarán por el uso de los medios y servicios compartidos. En este sentido, cuando las necesidades puedan ser comunes a más de un área funcional o unidad, del mismo o de distinto ministerio, se escogerá la alternativa que permita compartir el servicio entre dichas áreas, salvo autorización expresa de la Dirección de Tecnologías de la Información y las Comunicaciones.

7. La Dirección de Tecnologías de la Información y las Comunicaciones llevará un registro de los costes que son imputables a cada uno de los diferentes órganos y organismos usuarios, sin perjuicio de las competencias de otros órganos administrativos en materia de control de gasto.

8. La puesta a disposición común de los medios y servicios compartidos se hará de acuerdo con lo previsto en la normativa que resulte aplicable en cada ámbito en materia de personal, organización, presupuestos y patrimonial.

**Artículo 11.** *Proyectos de interés prioritario.*

El Comité de Estrategia TIC podrá declarar como proyectos de interés prioritario aquellos que tengan una singular relevancia y, especialmente, aquellos que tengan como objetivo la colaboración y cooperación con las comunidades autónomas y los entes que integran la Administración local y la Unión Europea en materia de Administración digital.

La declaración de proyecto de interés prioritario se trasladará como recomendación al Ministerio de Hacienda y Administraciones Públicas y a la Comisión de Políticas de Gasto para que, en su caso, sea tenida en cuenta en la elaboración de los Presupuestos Generales del Estado.

**Artículo 12.** *Unidades TIC.*

1. Son unidades TIC aquellas unidades administrativas cuya función sea la provisión de servicios en materia de Tecnologías de la Información y Comunicaciones a sí mismas o a otras unidades administrativas.

Las unidades TIC, bajo la dirección de los órganos superiores o directivos a los que se encuentren adscritas, se configuran como instrumentos fundamentales para la implementación y desarrollo de la Estrategia TIC y del proceso de transformación digital de los ámbitos sectoriales de la Administración General del Estado y sus Organismos Públicos bajo la coordinación y supervisión de la Dirección de Tecnologías de la Información y las Comunicaciones.

2. Se entenderá por provisión de servicios TIC la realización de una o varias de las siguientes funciones:

a) Soporte, operación, implementación y/o gestión de sistemas informáticos corporativos o de redes de telecomunicaciones.

b) Desarrollo de aplicativos informáticos en entornos multiusuario.

c) Consultoría informática.

d) Seguridad de sistemas de información.

e) Atención técnica a usuarios.

f) Innovación en el ámbito de las TIC

g) Administración digital.

h) Conformar la voluntad de adquisición de bienes o servicios en el ámbito de las tecnologías de la información y las comunicaciones

i) Todas aquellas funciones no previstas expresamente en las letras anteriores, que sean relevantes en materia de tecnologías de la información y las comunicaciones.

3. Las unidades TIC adscritas a los departamentos ministeriales o a sus organismos adscritos, impulsarán, en el marco de la CMAD, la transformación digital de los servicios sectoriales en sus ámbitos. La Dirección de Tecnologías de la Información y las Comunicaciones propondrá a los órganos competentes, las áreas administrativas que deban ser atendidas por las unidades TIC de manera que se adapten a las nuevas necesidades derivadas de la declaración de medios o servicios compartidos con el fin de mejorar la eficiencia y operatividad en la prestación de sus servicios. Las unidades TIC deberán llevar a cabo dicha transformación identificando las oportunidades que les permitan sacar el máximo

rendimiento a las TIC de acuerdo a las necesidades funcionales determinadas por las áreas administrativas a las que prestan sus servicios.

**Artículo 13.** *Cooperación interadministrativa.*

1. La Dirección de Tecnologías de la Información y las Comunicaciones propondrá a la Secretaría de Estado de Administraciones Públicas las líneas de actuación, orientaciones comunes y la creación de órganos de cooperación necesarios para favorecer el intercambio de ideas, estándares, tecnología y proyectos orientados a garantizar la interoperabilidad y mejorar la eficacia y eficiencia en la prestación de los servicios públicos de las distintas Administraciones Públicas, que serán tratadas en la Conferencia Sectorial de Administraciones Públicas, en cuyo seno se establecerán.

2. La Dirección de Tecnologías de la Información y las Comunicaciones propondrá al Secretario de Estado de Administraciones Públicas la designación de los representantes de la Administración General del Estado y sus Organismos Públicos en las comisiones o grupos que la Conferencia Sectorial de Administraciones Públicas cree en materia de tecnologías de la información y Administración digital.

## CAPÍTULO IV

## Actuaciones en relación con la planificación en materia de Administración digital

**Artículo 14.** *Planes de acción departamentales para la transformación digital.*

1. Cada ministerio contará con un Plan de acción para la transformación digital, que comprenderá las actuaciones en materia de Administración digital, tecnologías de la información y comunicaciones a desarrollar en el conjunto del departamento y sus organismos públicos adscritos.

2. La propuesta del plan se elaborará de acuerdo con las directrices de la Dirección de Tecnologías de la Información y las Comunicaciones y las líneas estratégicas establecidas por el Comité de Estrategia TIC y recogerá de forma concreta los servicios que el ministerio tiene previsto desarrollar, especialmente los dirigidos a la prestación de servicios a ciudadanos y empresas, su planificación temporal, los recursos humanos, técnicos y financieros necesarios y los contratos que se deben realizar.

La propuesta de plan de acción departamental se remitirá por el presidente de la CMAD a la Dirección de Tecnologías de la Información y las Comunicaciones para su estudio y valoración y posterior elevación a la Comisión de Estrategia de Tecnologías de la Información y las Comunicaciones, a efectos del informe preceptivo del Comité Ejecutivo, previo a su aprobación por el órgano competente en el departamento ministerial.

En el plan de acción remitido podrán excluirse los medios y servicios específicos que afecten a la defensa, consulta política, situaciones de crisis y seguridad del Estado y los que manejen información clasificada, de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales.

3. Los planes de acción para la trasformación digital tendrán un alcance, al menos, de dos años.

**Artículo 15.** *Modificación de los Planes de acción departamentales para la transformación digital.*

La modificación de los Planes de acción departamentales para la transformación digital deberá ser informada por la Dirección de Tecnologías de la Información y las Comunicaciones.

CAPÍTULO V

**Actuaciones en relación con la contratación en materia de tecnologías de la información**

**Artículo 16.** *Competencias para el informe técnico de la memoria y los pliegos de prescripciones técnicas para la contratación de tecnologías de la información.*

1. La Dirección de Tecnologías de la Información y las Comunicaciones elaborará y trasladará a los órganos competentes en materia de contratación, los criterios y directrices para la agregación y planificación de la demanda TIC en la Administración General del Estado y sus Organismos Públicos para una mayor eficiencia económica y su configuración como cliente único frente a proveedores externos.

2. La Dirección de Tecnologías de la Información y las Comunicaciones informará con carácter preceptivo la declaración de contratación centralizada, que corresponde al Ministro de Hacienda y Administraciones Públicas a propuesta de la Dirección General de Racionalización y Centralización de la Contratación, de los contratos de suministros, obras y servicios en materia TIC.

Asimismo, para la contratación centralizada en materia TIC la Dirección de Tecnologías de la Información y las Comunicaciones establecerá los criterios técnicos y de oportunidad y la Dirección General de Racionalización y Centralización de la Contratación establecerá los criterios de contratación administrativa y gestión económica.

La Dirección de Tecnologías de la Información y las Comunicaciones realizará el informe técnico preceptivo de la memoria y los pliegos de prescripciones técnicas de las siguientes contrataciones de bienes y servicios informáticos:

a) El suministro de equipos y programas para el tratamiento de la información, de acuerdo con lo establecido en el artículo 9.3 b) del texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre.

b) Los contratos de servicios, de acuerdo con lo establecido en el artículo 10 del texto refundido de la Ley de Contratos del Sector Público.

c) Los procedimientos especiales de adopción de tipo realizados al amparo del artículo 206 del texto refundido Ley de Contratos del Sector Público.

d) Los convenios de colaboración y encomiendas de gestión que incluyan la prestación de servicios en materia de tecnologías de la información, comunicaciones o Administración Digital en el ámbito de la Administración General del Estado y sus Organismos Públicos.

3. Estarán excluidos del informe técnico a que se refiere el apartado anterior los contratos comprendidos en el ámbito de aplicación de la Ley 24/2011, de 1 de agosto, de Contratos del sector público en los ámbitos de la defensa y de la seguridad, así como los tramitados de conformidad con el artículo 170.f) del texto refundido de la Ley de Contratos del Sector Público.

La Dirección de Tecnologías de la Información y las Comunicaciones recibirá la información necesaria sobre estas contrataciones a efectos estadísticos, de inventario y presupuestarios necesarios para el gobierno integral de las TIC. En cualquier caso, la recepción de la información se manejará y custodiará de acuerdo a la clasificación establecida y, en su caso, con lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales.

**Artículo 17.** *Tramitación telemática de los informes a la memoria y los pliegos de prescripciones técnicas.*

1. La tramitación de los informes técnicos se regulará mediante instrucción de la Dirección de Tecnologías de la Información y las Comunicaciones y se hará procurando el empleo de medios telemáticos en todas las fases del procedimiento.

2. La tramitación de los informes técnicos se realizará bajo los principios de simplicidad, celeridad y eficacia, y se racionalizarán los trámites administrativos para lograr su máxima sencillez y funcionalidad.

3. El informe técnico se emitirá en el plazo máximo de diez días hábiles posteriores al día en que la unidad TIC registró la documentación completa del expediente de contratación.

Si por causas justificadas el informe previsto en el apartado anterior no pudiera ser emitido en el plazo previsto, se comunicará telemáticamente al órgano solicitante indicando si puede proseguir el procedimiento de contratación o si el informe se considera determinante para la prosecución del procedimiento de contratación, de suscripción de convenio o atribución de encomienda de gestión. En el caso de que el informe se considere determinante se indicará en la comunicación el nuevo plazo en que será evacuado, que no podrá superar 5 días hábiles, transcurrido el cuál sin la emisión del informe podrá proseguir la tramitación del expediente.

4. Las Unidades TIC proporcionarán la información necesaria para mantener actualizado el sistema integral de seguimiento de contratación TIC que permita un análisis permanente de los contratos TIC.

**Artículo 18.** *Contenido del informe técnico sobre la memoria y los pliegos de prescripciones técnicas en materia de tecnologías de la información.*

1. El informe técnico de la memoria y de los pliegos de prescripciones técnicas en materia de tecnologías de la información se referirá a su adecuación a los planes estratégicos del departamento ministerial y a las directrices dictadas por la Dirección de Tecnologías de la Información y las Comunicaciones, así como a la finalidad y adecuación tecnológica de la prestación que se propone contratar.

2. El informe técnico tendrá en cuenta los elementos de la memoria y del pliego de prescripciones técnicas que contengan información relevante desde el punto de vista tecnológico y de los criterios para la transformación digital de los servicios.

**Artículo 19.** *Información presupuestaria.*

1. La Dirección de Tecnologías de la Información y las Comunicaciones tendrá información, en coordinación con las Comisiones Ministeriales de Administración Digital y la Dirección General de Presupuestos, de los recursos económicos destinados a los bienes y servicios TIC del conjunto de la Administración General del Estado y sus Organismos Públicos se informará trimestralmente a la Comisión de Estrategia TIC del estado de ejecución de dicho presupuesto.

2. La Dirección de Tecnologías de la Información y las Comunicaciones elaborará un informe anual detallado y desagregado de imputación de costes TIC.

**Disposición adicional primera.** *Supresión de órganos.*

A partir de la entrada en vigor de este real decreto quedan suprimidos el Consejo Superior de Administración Electrónica y las Comisiones Ministeriales de Administración Electrónica.

**Disposición adicional segunda.** *Modificación de referencias.*

1. Se entenderán referidas a la Comisión de Estrategia TIC y a las Comisiones Ministeriales de Administración Digital todas las alusiones que en la normativa vigente se hagan al Consejo Superior de Administración Electrónica y a las Comisiones Ministeriales de Administración Electrónica, respectivamente.

2. Sin perjuicio de lo anterior, todas las referencias al Consejo Superior de Administración Electrónica y a las Comisiones Ministeriales de Administración Electrónica que subsistan en la normativa vigente en relación a las competencias de contratación de estos órganos colegiados, se entenderán hechas a la Dirección de Tecnologías de la Información y las Comunicaciones.

3. Todos los comités técnicos, grupos de trabajo o ponencias especiales que hayan sido constituidos por acuerdo del Consejo Superior de Administración Electrónica o de su Comité Permanente quedarán asociados a la Dirección de Tecnologías de la Información y las Comunicaciones o a los órganos colegiados regulados en este real decreto, de acuerdo con sus funciones.

**Disposición adicional tercera.** *Régimen jurídico de los órganos colegiados.*

1. Los órganos colegiados que se regulan en este real decreto se regirán por lo establecido en materia de órganos colegiados en el capítulo II del título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

2. La Comisión de Estrategia TIC podrá aprobar las normas de régimen interno que estime procedentes para el mejor desarrollo de su trabajo.

**Disposición adicional cuarta.** *Representación del Ministerio de Defensa en los órganos con competencias en materia de Administración digital.*

Sin perjuicio de lo establecido en el artículo 5.1, la representación del Ministerio de Defensa en el Pleno de la Comisión de Estrategia TIC podrá ser asumida por el órgano superior de ese departamento que, de acuerdo con los reales decretos de estructura orgánica y de desarrollo de la misma, resulte competente en materia de Tecnologías de la Información y Comunicaciones.

Asimismo, sin perjuicio de lo establecido en el artículo 7.2, el citado órgano superior podrá asumir la presidencia de la Comisión Ministerial de Administración Digital del Ministerio de Defensa y, sin perjuicio de lo establecido en el artículo 8, podrá ser el responsable TIC, dentro de dicho órgano superior del Ministerio de Defensa, quien represente al departamento en el Comité de Dirección de las Tecnologías de Información y Comunicaciones.

**Disposición adicional quinta.** *Composición inicial del Comité Ejecutivo de la Comisión de Estrategia TIC.*

El Comité Ejecutivo de la Comisión de Estrategia TIC estará formado por los titulares de los siguientes órganos, en tanto que la Comisión de Estrategia TIC no establezca una composición diferente:

a) Dirección General de Racionalización y Centralización de la Contratación.
b) Dirección General de Presupuestos.
c) Dirección General de Telecomunicaciones y Tecnologías de la Información.
d) Gerencia de Informática de la Seguridad Social.
e) Departamento de Informática Tributaria de la Agencia Estatal de Administración Tributaria.
f) Secretaría General de la Administración de Justicia.
g) Dirección General de la Función Pública.
h) Inspección General del Ministerio de Hacienda y Administraciones Públicas.
i) Intervención General de la Administración del Estado.
j) Una Subdirección General del Centro Nacional de Inteligencia/Centro Criptológico Nacional.

**Disposición adicional sexta.** *Ámbito específico.*

Lo dispuesto en el presente real decreto será de aplicación a los organismos y entidades públicos no encuadrables en las categorías establecidas en el artículo 43.1 de la Ley 6/1997, de 14 de abril, de Organización y funcionamiento de la Administración General del Estado, en cuanto sea compatible con su normativa específica.

**Disposición transitoria primera.** *Expedientes de contratación en fase de informe.*

Se pospone hasta el 1 de enero de 2015 la entrada en vigor del nuevo procedimiento de tramitación de los informes de la memoria y de los pliegos de prescripciones técnicas.

Durante este periodo, los expedientes se seguirán tramitando por el procedimiento anterior, asumiendo directamente la Dirección de Tecnologías de la Información y las Comunicaciones la aprobación de los expedientes que hasta el momento eran competencia del Consejo Superior de Administración Electrónica.

Los expedientes que se inicien durante este periodo y los contratos adjudicados durante el mismo, así como los expedientes ya iniciados y los contratos adjudicados con anterioridad a la entrada en vigor de este real decreto se regirán de acuerdo con la normativa anterior. A estos efectos, se entenderá que los expedientes han sido iniciados cuando hayan sido remitidos a la Comisión Permanente del Consejo Superior de Administración Electrónica o a la correspondiente Comisión Ministerial de Administración Electrónica para su informe preceptivo o tramitación.

**Disposición transitoria segunda.** *Regulación de las Comisiones Ministeriales de Administración Digital.*

En el plazo de cuatro meses desde la entrada en vigor de este real decreto se aprobarán las correspondientes órdenes ministeriales reguladoras de las Comisiones Ministeriales de Administración Digital. Mientras tanto, subsistirán con su actual estructura las Comisiones Ministeriales de Administración Electrónica vigentes, que pasarán a ejercer las funciones que se atribuyen en este real decreto a las nuevas Comisiones Ministeriales de Administración Digital.

**Disposición derogatoria única.** *Derogación normativa.*

Queda derogado el Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados responsables de la Administración electrónica, así como cuantas disposiciones de igual o inferior rango se opongan a lo establecido en este real decreto.

**Disposición final primera.** *Facultades de desarrollo.*

Se autoriza a los Ministros de Hacienda y Administraciones Públicas y de la Presidencia, en el ámbito de sus respectivas competencias, para que adopten las medidas necesarias para el desarrollo y ejecución de este real decreto.

**Disposición final segunda.** *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

# § 3

## Ley 22/2021, de 28 de diciembre, de Presupuestos Generales del Estado para el año 2022. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 312, de 29 de diciembre de 2021
Última modificación: 30 de mayo de 2024
Referencia: BOE-A-2021-21653

[ . . . ]

**Disposición adicional centésima décima séptima.** *Creación de la Agencia Estatal de Administración Digital.*

Uno. De acuerdo con lo previsto en el artículo 91 de la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, se autoriza la creación de la Agencia Estatal de Administración Digital, como organismo público con personalidad jurídica pública y patrimonio propios y plena capacidad de obrar.

Dos. La actuación de la Agencia responderá a los siguientes fines:

a) La digitalización del sector público, mediante el ejercicio de las funciones de dirección, coordinación y ejecución del proceso de transformación digital e innovación de la Administración a través de las tecnologías de la información y de las comunicaciones.

b) La prestación eficiente de los servicios públicos, a través de la adopción de soluciones digitales, en el marco de los Esquemas Nacionales de Seguridad e Interoperabilidad.

c) La transformación digital de las Administraciones Públicas a través de la coordinación de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, y de la cooperación con las administraciones públicas para la implantación de las estrategias nacionales e internacionales en materia de administración digital.

d) La coordinación funcional de la actuación de las unidades TIC de la Administración General del Estado y el apoyo informático a aquellos departamentos ministeriales que lo precisen.

Tres. De acuerdo con los fines enunciados, corresponderá a la Agencia el impulso en la definición, desarrollo, ejecución y seguimiento, entre otros, de los proyectos de transformación digital incluidos el Plan de Digitalización de las Administraciones Públicas 2021-2025 para mejorar la accesibilidad de los servicios públicos digitales a la ciudadanía y empresas, superar la actual brecha digital y favorecer la eficiencia y eficacia de los empleados públicos, avanzando hacia una Administración del siglo XXI y contribuyendo a la consecución de objetivos de resiliencia y transición digital perseguidos también por el Plan Nacional de Recuperación, Transformación y Resiliencia.

Esto se llevará a cabo mediante la ejecución, entre otras actuaciones, de las medidas incluidas en el Plan de Digitalización de las Administraciones Públicas 2021-2025.

Cuatro. Estará adscrita a la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital. Se regirá por lo establecido en su estatuto orgánico y por lo dispuesto en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Cinco. La asistencia jurídica, consistente en el asesoramiento y la representación y defensa en juicio de la Agencia, corresponderá a los Abogados del Estado integrados en el Servicio Jurídico del Estado.

[ . . . ]

# § 4

# Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público

Jefatura del Estado
«BOE» núm. 276, de 17 de noviembre de 2007
Última modificación: 9 de mayo de 2023
Referencia: BOE-A-2007-19814

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

## PREÁMBULO

La información generada desde las instancias públicas, con la potencialidad que le otorga el desarrollo de la sociedad de la información, posee un gran interés para las empresas a la hora de operar en sus ámbitos de actuación, contribuir al crecimiento económico y la creación de empleo, y para los ciudadanos como elemento de transparencia y guía para la participación democrática. Recogiendo ambas aspiraciones la Directiva 2003/98/CE, de 17 de noviembre de 2003, del Parlamento Europeo y del Consejo, relativa a la reutilización de la información del sector público, se adoptó con la finalidad de explotar el potencial de información del sector público y superar las barreras de un mercado europeo fragmentado estableciendo unos criterios homogéneos, asentados en condiciones equitativas, proporcionadas y no discriminatorias para el tratamiento de la información susceptible de ser reutilizada por personas físicas o jurídicas.

Las diferentes Administraciones y organismos del sector público recogen, producen, reproducen y difunden documentos para llevar a cabo la misión de servicio público que tienen encomendada. Como expresa la Directiva 2003/98/CE, la utilización de dichos documentos por otros motivos, ya sea con fines comerciales o no comerciales, constituye una reutilización. Por una parte, se persigue armonizar la explotación de la información en el sector público, en especial la información en soporte digital recopilada por sus distintos organismos relativa a numerosos ámbitos de interés como la información social, económica, jurídica, geográfica, meteorológica, turística, sobre empresas, patentes y educación, etc., al objeto de facilitar la creación de productos y servicios de información basados en documentos del sector público, y reforzar la eficacia del uso transfronterizo de estos documentos por parte de los ciudadanos y de las empresas privadas para que ofrezcan productos y servicios de información de valor añadido. Por otra parte, la publicidad de todos los documentos de libre disposición que obran en poder del sector público referentes no sólo

a los procedimientos políticos, sino también a los judiciales, económicos y administrativos, es un instrumento esencial para el desarrollo del derecho al conocimiento, que constituye un principio básico de la democracia.

Estos objetivos son los que persigue la presente ley, que mediante la incorporación a nuestro ordenamiento jurídico de la Directiva 2003/98/CE y, tomando como punto de partida el diverso tratamiento que las Administraciones y organismos del sector público han otorgado a la explotación de la información, dispone un marco general mínimo para las condiciones de reutilización de los documentos del sector público que acoja las diferentes modalidades que se pueden adoptar y que dimanan de la heterogeneidad de la propia información. En consecuencia, se prevé que sean las Administraciones y organismos del sector público los que decidan autorizar o no la reutilización de los documentos o categorías de documentos por ellos conservados con fines comerciales o no comerciales. Asimismo, se pretende promover la puesta a disposición de los documentos por medios electrónicos, propiciando el desarrollo de la sociedad de la información.

La ley posee unos contornos específicos que la delimitan del régimen general de acceso previsto en el artículo 105 b) de la Constitución Española y en su desarrollo legislativo, en esencia representado por la Ley 30/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En este sentido resulta necesario precisar que no se modifica el régimen de acceso a los documentos administrativos consagrado en nuestro ordenamiento jurídico, sino que se aporta un valor añadido al derecho de acceso, contemplando el marco de regulación básico para la explotación de la información que obra en poder del sector público, en un marco de libre competencia, regulando las condiciones mínimas a las que debe acogerse un segundo nivel de tratamiento de la información que se genera desde las instancias públicas.

En el Título I de la ley se prevé el ámbito subjetivo de aplicación, que se extiende a las Administraciones y organismos del sector público en el sentido definido en su artículo 2, en consonancia con la delimitación realizada en la normativa de contratación del sector público. Desde la perspectiva de su aplicación objetiva, la ley contempla una definición genérica del término documento, acorde con la evolución de la sociedad de la información y que engloba todas las formas de representación de actos, hechos o información, y cualquier recopilación de los mismos, independientemente del soporte (escrito en papel, almacenado en forma electrónica o como grabación sonora, visual o audiovisual) conservados por las Administraciones y organismos del sector público, e incluye una delimitación negativa del ámbito de aplicación, enumerando aquellos documentos o categorías de documentos que no se encuentran afectados por la misma, atendiendo a diversos criterios. En este punto cabe precisar que la ley no se aplica a los documentos sometidos a derechos de propiedad intelectual o industrial (como las patentes, los diseños y las marcas registradas) especialmente por parte de terceros. A los efectos de esta ley se entiende por derechos de propiedad intelectual los derechos de autor y derechos afines, incluidas las formas de protección sui géneris. En este sentido, la ley tampoco afecta a la existencia de derechos de propiedad intelectual de las Administraciones y organismos del sector público, ni restringe en modo alguno el ejercicio de esos derechos fuera de los límites establecidos en su articulado. Las obligaciones impuestas por esta ley sólo deben aplicarse en la medida en que resulten compatibles con las disposiciones de los acuerdos internacionales sobre protección de los derechos de propiedad intelectual, en particular el Convenio de Berna para la protección de las obras literarias y artísticas (Convenio de Berna) y el Acuerdo sobre aspectos de los derechos de propiedad intelectual relacionados con el comercio (Acuerdo ADPIC). No obstante, las instancias públicas deben ejercer sus derechos de autor de una manera que facilite la reutilización.

El Título II prevé los aspectos básicos del régimen jurídico de la reutilización, indicando que las Administraciones y organismos del sector público podrán optar por permitir la reutilización sin condiciones concretas o, mediante la expedición de una licencia, que imponga a su titular una serie de condiciones de reutilización que, en todo caso, deberán ser claras, justas y transparentes, no discriminatorias para categorías comparables de reutilización y atender al principio de libre competencia y de servicio público.

Para ello el uso de licencias-tipo que puedan estar disponibles por medios electrónicos se revela como un elemento clave en este sentido. Por otra parte, se prevé que las distintas

Administraciones y organismos difundan qué documentación es susceptible de ser reutilizada mediante la creación de listados e índices accesibles en línea de los documentos disponibles, con el objeto de fomentar y facilitar las solicitudes de reutilización. Para incrementar las posibilidades de reutilización, las Administraciones y organismos del sector público deben procurar ofrecer los documentos por medios electrónicos en los formatos o lenguas preexistentes.

El régimen de reutilización garantiza el pleno respeto de los principios que consagran la protección de datos personales, en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y su normativa de desarrollo.

Por otra parte, las Administraciones y organismos del sector público deben adecuarse a las normas de competencia, evitando acuerdos exclusivos. No obstante, la ley prevé una excepción a este principio cuando, con vistas a la prestación de un servicio de interés económico general, pueda resultar necesario conceder un derecho exclusivo a la reutilización de determinados documentos del sector público.

Asimismo, la ley prevé los principios aplicables para aquellos supuestos en los que las Administraciones y organismos exijan contraprestaciones económicas por facilitar la reutilización de documentos con fines comerciales, cuya cuantía deberá ser razonable y orientada al coste, sin que los ingresos obtenidos superen los costes totales de recogida, producción, reproducción y difusión de los documentos.

En el Título II se concretan algunos aspectos de la reutilización de la información, previendo las posibles condiciones a las que someter la reutilización, que podrían ir referidas a cuestiones como el uso correcto de los documentos, la garantía de que los documentos no serán modificados y la indicación de la fuente. Asimismo se indica el contenido mínimo que deben acoger las licencias.

En el Título III la ley establece el procedimiento para poder arbitrar las solicitudes de reutilización, en el que tienen una especial relevancia los plazos de resolución, aspecto esencial para el contenido dinámico de la información, cuyo valor económico depende de su puesta a disposición inmediata y de una actualización regular. Asimismo se garantiza que en las resoluciones que se adopten se indiquen las vías de recurso de las que disponen los solicitantes para impugnar las decisiones que les afecten.

Por último se establece para la Administración General del Estado un régimen sancionador conectado con el mal uso que se confiera a la información cuya reutilización ha sido autorizada.

La presente Ley tiene carácter de legislación básica al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución. Se exceptúa el artículo 11 y los apartados 1 (párrafos segundo y tercero), 3 y 8 del artículo 10.

En la elaboración de la ley se ha recabado el informe de la Agencia Española de Protección de Datos.

## TÍTULO I

## Disposiciones generales

**Artículo 1.** *Objeto.*

La presente ley tiene por objeto la regulación básica del régimen jurídico aplicable a la reutilización de los documentos elaborados o custodiados por los sujetos incluidos en el ámbito subjetivo de aplicación regulado en el artículo 2, así como de los datos de investigación de acuerdo con las condiciones establecidas en el artículo 3.bis.

La aplicación de esta ley se hará sin perjuicio del régimen aplicable al derecho de acceso a los documentos y a las especialidades previstas en su normativa reguladora.

**Artículo 2.** *Ámbito subjetivo de aplicación.*

La presente Ley se aplica a:

a) La Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local.

b) Los organismos y entidades del sector público institucional creados para satisfacer necesidades de interés general, que no tengan carácter industrial o mercantil.

c) Las sociedades mercantiles pertenecientes al sector público institucional que:

1.º Lleven a cabo su actividad en los ámbitos definidos en la Directiva 2014/25/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la contratación por entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales y por la que se deroga la Directiva 2004/17/CE Texto pertinente a efectos del EEE.

2.º Actúen como operadores de servicio público con arreglo al artículo 2 del Reglamento (CE) n.º 1370/2007 del Parlamento Europeo y del Consejo, de 23 de octubre de 2007, sobre los servicios públicos de transporte de viajeros por ferrocarril y carretera y por el que se derogan los Reglamentos (CEE) n.º 1191/69 y (CEE) n.º 1107/70 del Consejo.

3.º Actúen como compañías aéreas que cumplen obligaciones de servicio público con arreglo al artículo 16 del Reglamento (CE) n.º 1008/2008 del Parlamento Europeo y del Consejo, de 24 de septiembre de 2008, sobre normas comunes para la explotación de servicios aéreos en la Comunidad.

4.º Actúen como armadores comunitarios que cumplen obligaciones de servicio público con arreglo al artículo 4 del Reglamento (CEE) n.º 3577/92 del Consejo, de 7 de diciembre de 1992, por el que se aplica el principio de libre prestación de servicios a los transportes marítimos dentro de los Estados miembros (cabotaje marítimo).

**Artículo 3.** *Ámbito objetivo de aplicación.*

1. Se entiende por reutilización el uso por personas físicas o jurídicas de documentos elaborados o custodiados por:

a) Los sujetos previstos en los párrafos a) y b) del artículo 2, con fines comerciales o no comerciales distintos del propósito inicial que tenían esos documentos en la actividad de servicio público para la que se produjeron, excepto para el intercambio de documentos entre dichos sujetos en el marco de sus actividades de servicio público.

b) Las sociedades mercantiles públicas a que se refiere el párrafo c) del artículo 2 con fines comerciales o no comerciales distintos del propósito inicial que tenían esos documentos de prestar servicios de interés general para el que se produjeron, excepto para el intercambio de documentos entre estas sociedades mercantiles públicas y el resto de sujetos previstos en el artículo 2 que se realice exclusivamente en el desarrollo de las actividades de servicio público de estos últimos.

2. Esta ley se aplica, asimismo, a los datos de investigación en los términos previstos en el artículo 3.bis y a los documentos a los que se aplica la Directiva 2007/2/CE del Parlamento Europeo y del Consejo, de 14 de marzo de 2007, por la que se establece una infraestructura de información espacial en la Comunidad Europea (Inspire).

3. Esta ley no será aplicable a los siguientes documentos elaborados o custodiados por los sujetos previstos en el artículo 2:

a) Los documentos sobre los que existan prohibiciones o limitaciones en el derecho de acceso en virtud de lo previsto en el artículo 13 de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y las demás normas que regulan el derecho de acceso o la publicidad registral con carácter específico.

b) De conformidad con su legislación específica, los documentos que afecten a la defensa nacional, la seguridad del Estado, la protección de la seguridad pública, así como los obtenidos por la Administración Tributaria y la Administración de la Seguridad Social en el desempeño de sus funciones, los sometidos al secreto estadístico, a la confidencialidad comercial, tales como secretos comerciales, profesionales o empresariales y, en general, los documentos relacionados con actuaciones sometidas por una norma al deber de reserva, secreto o confidencialidad.

c) Los documentos para cuyo acceso se requiera ser titular de un derecho o interés legítimo.

d) Los documentos que obran en poder de los sujetos previstos en los párrafos a) y b) del artículo 2 para finalidades ajenas a las funciones de servicio público de acuerdo con la legislación aplicable y en particular, con la normativa de creación del servicio público de que se trate.

e) Los documentos sobre los que existan derechos de propiedad intelectual o industrial por parte de terceros.

No obstante, esta ley no afecta a la existencia de derechos de propiedad intelectual de los sujetos previstos en el artículo 2 ni a su posesión por éstos, ni restringe el ejercicio de esos derechos fuera de los límites establecidos por esta ley. El ejercicio de los derechos de propiedad intelectual de los sujetos previstos en el artículo 2 deberá realizarse de forma que se facilite su reutilización.

Lo previsto en el párrafo anterior será de aplicación, asimismo, a los documentos respecto de los que las bibliotecas, incluidas las universitarias, los museos y los archivos sean titulares originarios de los derechos de propiedad intelectual como creadores de la misma conforme a lo establecido en la legislación de propiedad intelectual, así como cuando sean titulares porque se les haya transmitido la titularidad de los derechos sobre dicha obra según lo dispuesto en la citada legislación, debiendo en este caso respetar lo establecido en los términos de la cesión.

f) Los documentos conservados por las entidades que gestionen los servicios esenciales de radiodifusión sonora y televisiva y sus filiales.

g) Los documentos conservados por instituciones educativas de nivel secundario e inferior y, en el caso de todas las demás instituciones educativas, documentos distintos de los datos investigación referidos en el artículo 1.

h) Los documentos distintos de los datos de investigación mencionados en el artículo 1, conservados por organizaciones que realizan actividades de investigación y organizaciones que financian la investigación, incluidas las organizaciones creadas para la transferencia de los resultados de la investigación.

i) Los documentos producidos o conservados por instituciones culturales que no sean bibliotecas, incluidas las universitarias, museos y archivos.

j) Los logotipos, divisas e insignias.

k) Los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de los datos personales, de conformidad con la normativa vigente y las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales.

l) Los documentos elaborados por entidades del sector público empresarial, excepto las previstas en el párrafo c) del artículo 2, y fundacional en el ejercicio de las funciones atribuidas legalmente y los de carácter comercial, industrial o mercantil elaborado en ejecución del objeto social previsto en sus Estatutos.

m) Los estudios realizados por entidades del sector público en colaboración con el sector privado, mediante convenios o cualquier otro tipo de instrumento, como fórmula de financiación de los mismos.

n) Los documentos cuyo acceso esté excluido o limitado por motivos de protección de información sensible sobre infraestructuras críticas.

ñ) Los documentos producidos o conservados por las sociedades mercantiles públicas previstas en el párrafo c) del artículo 2, fuera del ámbito de la prestación de servicios de interés general o relativos a actividades sometidas directamente a la competencia y no sujetas a la normativa de contratación de entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales.

4. En ningún caso, podrá ser objeto de reutilización, la información en que la ponderación a la que se refieren los artículos 5.3 y 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, arroje como resultado la prevalencia del derecho fundamental a la protección de datos de carácter personal, a menos que se produzca la disociación de los datos a la que se refiere el artículo 15.4 de la citada Ley.

**Artículo 3.bis.** *Datos de investigación.*

1. Las entidades incluidas en el ámbito de aplicación del artículo 2 de la presente Ley y que realicen actividades de investigación o financien la investigación adoptarán medidas para apoyar que los datos de investigaciones financiadas públicamente sean plenamente reutilizables, interoperables y de acceso abierto, teniendo en cuenta las limitaciones que pudieran derivarse de los derechos de propiedad intelectual e industrial, la protección de datos personales y la confidencialidad, la seguridad y los intereses comerciales legítimos.

2. Sin perjuicio de lo previsto en el artículo 3.3.e) y de los intereses comerciales legítimos, las actividades de transferencia de conocimientos y los derechos de propiedad intelectual preexistentes, los datos de investigación serán reutilizables para fines comerciales o no comerciales, de conformidad con lo dispuesto en la presente Ley, cuando sean financiados con fondos públicos y cuando los investigadores, las universidades o las organizaciones que realizan actividades de investigación o que financien la investigación ya hubieran puesto tales datos a disposición del público a través de un repositorio institucional o temático y, en todo caso, con pleno respeto a la normativa vigente en materia de propiedad intelectual.

**Artículo 3.ter.** *Conjuntos de datos de alto valor.*

1. Además de la lista de conjuntos de datos específicos de alto valor que, en su caso, establezca la Comisión Europea, se podrán determinar a nivel nacional otros conjuntos de datos adicionales seleccionados en relación a su potencial para generar beneficios socioeconómicos o medioambientales importantes y servicios innovadores; beneficiar a un gran número de usuarios, en concreto pymes; contribuir a generar ingresos, y la posibilidad de ser combinados con otros conjuntos de datos.

2. Dichos conjuntos de datos de alto valor, tanto los establecidos a nivel europeo como nacional:

a) Estarán disponibles gratuitamente, a reserva de lo previsto en el artículo 7.9.a).
b) Serán legibles por máquina
c) Se suministrarán a través de interfaz de programación de aplicaciones (API), y
d) Se proporcionarán en forma de descarga masiva, cuando proceda.

Se podrán especificar acuerdos organizativos relativos a la publicación y de reutilización de los tipos de conjuntos de datos de alto valor. Esos acuerdos serán compatibles con las licencias tipo abiertas. Los acuerdos podrán incluir condiciones aplicables a la reutilización, el formato de los datos y los metadatos, así como acuerdos técnicos para la difusión.

3. El Ministerio de Asuntos Económicos y Transformación Digital aprobará la lista de los conjuntos de datos de alto valor nacionales que se publicará mediante Resolución de la Secretaria de Estado de Digitalización e Inteligencia Artificial. La selección y actualización de los conjuntos de datos incluidos en dicha lista se realizará a través de la División Oficina del Dato contando con la colaboración de los actores interesados, tanto públicos como privados, a través de los órganos y mecanismos que se establezcan.

## TÍTULO II

## Régimen jurídico de la reutilización

**Artículo 4.** *Régimen administrativo de la reutilización.*

1. Los documentos de los sujetos previstos en el artículo 2 serán reutilizables en los términos previstos en esta ley. Dichos sujetos velarán porque los documentos a los que se aplica esta normativa puedan ser reutilizados para fines comerciales o no comerciales de conformidad con alguna o algunas de las siguientes modalidades:

a) Reutilización de documentos puestos a disposición del público sin sujeción a condiciones.
b) Reutilización de documentos puestos a disposición del público con sujeción a condiciones establecidas en licencias-tipo.

c) Reutilización de documentos previa solicitud, conforme al procedimiento previsto en el artículo 10 o, en su caso, en la normativa autonómica, pudiendo incorporar en estos supuestos condiciones establecidas en una licencia.

d) Acuerdos exclusivos conforme el procedimiento previsto en el artículo 6.

2. La reutilización de documentos no estará sujeta a condiciones a menos que estas sean objetivas, proporcionadas, no discriminatorias y estén justificadas por un objetivo de interés público. En los supuestos de sujeción, las condiciones se fijarán en una licencia.

Los sujetos previstos en el artículo 2 podrán facilitar licencias-tipo para la reutilización de documentos, las cuales deberán estar disponibles en formato digital y ser procesables electrónicamente.

3. Las condiciones incorporadas en las licencias habrán de respetar los siguientes criterios:

a) Deberán ser claras, justas y transparentes.

b) No deberán restringir las posibilidades de reutilización ni limitar la competencia.

c) No deberán ser discriminatorias para categorías comparables de reutilización, incluida la reutilización transfronteriza.

4. Los sujetos a que se refieren los párrafos a) y b) del artículo 2 no ejercerán el derecho del fabricante de una base de datos previsto en el artículo 133 de la Ley 5/1998, de 6 de marzo, de incorporación al Derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, sobre la protección jurídica de las bases de datos, para evitar la reutilización de documentos o restringir la reutilización más allá de los límites establecidos en esta Ley.

5. Los sujetos previstos en el artículo 2 crearán dispositivos y sistemas de gestión documental que permitan a los ciudadanos una recuperación eficaz de la información, disponible en línea y que enlacen con los dispositivos y sistemas de gestión puestos a disposición por otras Administraciones. Asimismo, facilitarán herramientas informáticas que permitan el acceso en línea a los listados de los documentos que puedan ser ampliamente reutilizables y la búsqueda de los documentos disponibles para su reutilización, con los metadatos pertinentes de conformidad con lo establecido en las normas técnicas de interoperabilidad, accesibles, siempre que sea posible y apropiado, en línea y en formato legible por máquina.

Los sujetos previstos en los párrafos a) y b) del artículo 2 promoverán la creación de sistemas que permitan la conservación de los documentos disponibles para su reutilización.

La Administración General del Estado mantendrá el catálogo nacional de información pública reutilizable en el que se pondrán a disposición los conjuntos de datos relativos a los documentos a los que aplica la presente Ley, en formatos accesibles, fáciles de localizar y reutilizables. Este catálogo dará cobertura, al menos, al ámbito de la Administración General del Estado y a sus organismos y entidades de derecho público vinculados o dependientes. Los posibles catálogos de información pública reutilizable establecidos por el resto de sujetos previstos en el artículo 2 deberán interoperar con el catálogo nacional cumpliendo las Normas Técnicas de Interoperabilidad que se establezcan al respecto.

Los catálogos de información pública reutilizable proporcionarán información sobre los derechos previstos en esta ley y ofrecerán la ayuda pertinente.

En la medida de lo posible, se facilitará la búsqueda multilingüe de los documentos, en particular permitiendo la agregación de metadatos a escala de la Unión Europea.

6. La reutilización de documentos que contengan datos de carácter personal se regirá por lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

7. La utilización de los conjuntos de datos se realizará por parte de los usuarios o agentes de la reutilización bajo su responsabilidad y riesgo, correspondiéndoles en exclusiva a ellos responder frente a terceros por daños que pudieran derivarse de ella.

Los sujetos previstos en el artículo 2 no serán responsables del uso que de su información hagan los agentes reutilizadores ni tampoco de los daños sufridos o pérdidas económicas que, de forma directa o indirecta, produzcan o puedan producir perjuicios económicos, materiales o sobre datos, provocados por el uso de la información reutilizada.

8. La puesta a disposición de un documento para su reutilización no supone renuncia al derecho a su explotación, ni es impedimento para la modificación de los datos que en el mismo consten como consecuencia del ejercicio de funciones o competencias de dicho sujeto.

9. Igualmente, no se podrá indicar, de ningún modo, que los sujetos previstos en el artículo 2 pertenecientes al ámbito estatal titulares de la información reutilizada participan, patrocinan o apoyan la reutilización que se lleve a cabo de ella.

**Artículo 5.** *Formatos disponibles para la reutilización.*

1. La elaboración y la puesta a disposición de los documentos incluidos en el ámbito de aplicación de la presente Ley se efectuará, en la medida de lo posible, conforme al principio de documentos abiertos desde el diseño y por defecto.

2. Los sujetos previstos en el artículo 2 promoverán que la puesta a disposición de los documentos para su reutilización, así como que la tramitación de solicitudes de reutilización se realice por medios electrónicos y mediante plataforma multicanal cuando ello sea compatible con los medios técnicos de que disponen.

3. Los sujetos previstos en el artículo 2 facilitarán sus documentos en cualquier formato o lengua preexistente, pero también procurarán, siempre que ello sea posible y apropiado, proporcionarlos en formato abierto, accesible, legible por máquina conforme a lo previsto en el apartado anterior y conjuntamente con sus metadatos, con los niveles más elevados de precisión y desagregación, fáciles de localizar y reutilizables. Tanto el formato como los metadatos, en la medida de lo posible, deben cumplir estándares y normas formales abiertas. Esto no implicará que estén obligados a crear documentos, adaptarlos o facilitar extractos de documentos, cuando ello suponga un esfuerzo desproporcionado que conlleve algo más que una simple manipulación.

4. Los sujetos previstos en el artículo 2 pondrán a disposición los datos dinámicos de los que dispongan para su reutilización inmediatamente después de su recopilación, a través de interfaces de programación de aplicaciones (API) adecuadas y, cuando proceda, en forma de descarga masiva.

Cuando la puesta a disposición de datos dinámicos para su reutilización inmediatamente después de su recopilación pueda superar sus capacidades financieras o técnicas suponiendo un esfuerzo desproporcionado, esos datos dinámicos se pondrán a disposición para su reutilización en un plazo o con restricciones técnicas temporales que no perjudiquen indebidamente su potencial económico y social.

5. Los conjuntos de datos de alto valor, conforme al artículo 3 ter, que obren en poder de los sujetos previstos en el artículo 2 se pondrán a disposición para su reutilización en un formato legible por máquina, a través de interfaces de programación de aplicaciones adecuadas y, cuando proceda, en forma de descarga masiva.

6. Con arreglo a la presente Ley, no podrá exigirse a los sujetos previstos en el artículo 2 que mantengan la producción y el almacenamiento de un determinado tipo de documento con vistas a su reutilización.

7. Sin perjuicio de las definiciones establecidas en el Anexo, la puesta a disposición de los documentos para su reutilización por medios electrónicos por parte de los sujetos previstos en el artículo 2 debe realizarse en los términos establecidos por las normas reguladoras de la Administración electrónica, la interoperabilidad y los datos abiertos.

8. Con arreglo a lo establecido en el texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por el Real Decreto Legislativo 1/2013, de 29 de noviembre, los medios electrónicos de puesta a disposición de los documentos a que se refiere el apartado 2 de este artículo serán accesibles a las personas con discapacidad, de acuerdo con las normas técnicas existentes en la materia.

Asimismo, los sujetos previstos en el artículo 2 adoptarán, en lo posible, las medidas adecuadas para facilitar que aquellos documentos destinados a personas con discapacidad estén disponibles en formatos que tengan en cuenta las posibilidades de reutilización por parte de dichas personas.

No regirá esta obligación en los supuestos en los que dicha adecuación no constituya un ajuste razonable, entendiéndose por tal lo dispuesto en el artículo 7 del texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social.

**Artículo 6.** *Prohibición de derechos exclusivos.*

1. La reutilización de documentos estará abierta a todos los agentes potenciales del mercado, incluso en caso de que uno o más de los agentes exploten ya productos con valor añadido basados en estos documentos.

Los contratos o acuerdos de otro tipo entre los sujetos previstos en el artículo 2 que conserven los documentos y los terceros no otorgarán derechos exclusivos, sin perjuicio de lo previsto en los siguientes apartados.

2. Solo será admisible la suscripción de acuerdos exclusivos que corresponda a los mencionados sujetos a favor de terceros cuando tales derechos exclusivos sean necesarios para la prestación de un servicio de interés público. En tal caso, el sujeto previsto en el artículo 2 de que se trate quedará obligado a la realización de una revisión periódica, y en todo caso, cada tres años, con el fin de determinar si permanece la causa que justificó la concesión del mencionado derecho exclusivo. Estos acuerdos exclusivos deberán ser transparentes y públicos, debiendo ser puestos a disposición del público en línea al menos dos meses antes de su entrada en vigor.

3. Excepcionalmente, cuando exista un acuerdo exclusivo relacionado con la digitalización de los recursos culturales, el período de exclusividad no será superior, por regla general, a diez años. En el caso de que lo sea, su duración se revisará durante el undécimo año y, si procede, cada siete años a partir de entonces. Tales acuerdos deberán ser transparentes y se pondrán en conocimiento del público.

Cuando exista un acuerdo exclusivo en el sentido establecido en el párrafo anterior deberá facilitarse gratuitamente al sujeto de que se trate previsto en los párrafos a) y b) del artículo 2, como parte de dichos acuerdos, una copia de los recursos culturales digitalizados de la misma calidad y características técnicas del original, tales como formato, resolución, gama de colores, etc., con sus metadatos y requisitos técnicos de digitalización establecidos en la normas nacionales e internacionales pertinentes. Esa copia estará disponible para su reutilización una vez finalizado el período de exclusividad.

4. Los acuerdos que, sin conceder expresamente un derecho exclusivo, conlleven una disponibilidad limitada para la reutilización de documentos por entidades distintas de quienes participen en el acuerdo, deberán ser transparentes y públicos, siendo sus condiciones finales puestas a disposición del público en línea al menos dos meses antes de su entrada en vigor. El efecto de estos acuerdos sobre la disponibilidad de datos para su reutilización estará sujeto a revisiones periódicas y, en todo caso, se someterá a revisión cada tres años.

**Artículo 7.** *Tarifas.*

1. La reutilización de los documentos será gratuita. No obstante, podrá aplicarse una tarifa por el suministro de documentos para su reutilización en las condiciones previstas en la normativa estatal vigente o, en su caso, en la normativa que resulte de aplicación en el ámbito autonómico o local, limitándose la misma a los costes marginales en que se incurra para su reproducción, puesta a disposición, difusión, anonimización de datos personales y las medidas adoptadas para proteger información comercial confidencial.

En caso de que un sujeto previsto en el artículo 2 reutilice los documentos como base para actividades comerciales ajenas a las funciones propias que tenga atribuidas, deberán aplicarse a la entrega de documentos para dichas actividades las mismas tarifas y condiciones que se apliquen a los demás usuarios.

2. Lo dispuesto en el apartado anterior no se aplicará a:

a) Los sujetos previstos en el párrafo b) del artículo 2 a los que se exija generar ingresos para cubrir una parte sustancial de sus costes relativos a la realización de sus misiones de servicio público.

b) Las bibliotecas, incluidas las universitarias, los museos y los archivos.

c) Las sociedades mercantiles públicas a que se refiere párrafo c) del artículo 2.

3. Se publicará en línea una lista de los sujetos a los que se refiere la letra a) del apartado anterior.

4. En los casos a los que se refieren los párrafos a) y c) del apartado 2, se calculará el precio total conforme a criterios objetivos, transparentes y comprobables, que serán fijados mediante la normativa que corresponda. Los ingresos totales de cada sujeto obtenidos por

suministrar documentos y autorizar su reutilización durante el ejercicio contable apropiado no superarán el coste de recogida, producción, reproducción, difusión y almacenamiento de datos, incrementado por un margen de beneficio razonable de la inversión y, en su caso, anonimización de datos personales y medidas adoptadas para proteger la información comercial confidencial. La tarifa se calculará conforme a los principios contables aplicables y de acuerdo con la normativa aplicable.

5. Cuando quienes apliquen tarifas sean los sujetos mencionados en el párrafo b) del apartado 2, los ingresos totales obtenidos por suministrar y autorizar la reutilización de documentos durante el ejercicio contable apropiado no superarán el coste de recogida, producción, reproducción, difusión, almacenamiento de datos, conservación, compensación de derechos y, en su caso, anonimización de datos personales y medidas adoptadas para proteger la información comercial confidencial, incrementado por un margen de beneficio razonable de la inversión. A efectos de calcular dicho margen, estos sujetos podrán tener en cuenta los precios aplicados por el sector privado por la reutilización de documentos idénticos o similares. Las tarifas se calcularán conforme a los principios contables aplicables a los sujetos correspondientes y de acuerdo con la normativa aplicable.

6. Se podrán aplicar tarifas diferenciadas según se trate de reutilización con fines comerciales o no comerciales.

7. Los sujetos previstos en el artículo 2 publicarán por medios electrónicos, siempre que sea posible y apropiado, las tarifas fijadas para la reutilización de documentos que estén en su poder, así como las condiciones aplicables y el importe real de los mismos, incluida la base de cálculo utilizada.

En el resto de los casos en que se aplique una tarifa, el sujeto de que se trate indicará por adelantado qué factores se tendrán en cuenta para el cálculo de la misma. Cuando se solicite, dicho sujeto también indicará cómo se ha calculado esa tarifa en relación con la solicitud de reutilización concreta.

8. Cuando las tarifas a exigir tengan la naturaleza de tasa, su establecimiento y la regulación de sus elementos esenciales se ajustarán a lo previsto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, y demás normativa tributaria.

9. En todo caso, los usuarios podrán reutilizar gratuitamente:

a) Los conjuntos de datos de alto valor mencionados en el artículo 3 ter salvo que:

1.º) Se trate de documentos de bibliotecas, incluidas las universitarias, los museos y los archivos.

2.º) Se trate de documentos en poder de sociedades mercantiles públicas previstas en el párrafo c) del artículo 2, cuando el hecho de poner a disposición dichos conjuntos de datos de manera gratuita pudiera provocar una distorsión de la competencia en los mercados correspondientes.

3.º) Cuando el hecho de poner a disposición de forma gratuita conjuntos de datos de alto valor pueda tener un impacto sustancial en el presupuesto de organismos o entidades de derecho público que deban obtener ingresos para financiar su actividad de servicio público, en cuyo caso la Administración Pública a la que estén vinculados o de la que dependan podrá eximir a tales organismos o entidades de la obligación de poner a disposición de forma gratuita los conjuntos de datos de alto valor, por un período no superior a los dos años a partir de la entrada en vigor del acto de ejecución o resolución que apruebe la lista de conjuntos de datos de alto valor.

b) Los datos de investigación previstos en el artículo 1 de esta ley.

**Artículo 8.** *Condiciones de reutilización.*

La reutilización de la información de los sujetos previstos en el artículo 2 podrá estar sometida, entre otras, a las siguientes condiciones generales:

a) Que el contenido de la información, incluyendo sus metadatos, no sea alterado.
b) Que no se desnaturalice el sentido de la información.
c) Que se cite la fuente.
d) Que se mencione la fecha de la última actualización.

e) Cuando la información contenga datos de carácter personal, la finalidad o finalidades concretas para las que es posible la reutilización futura de los datos.

f) Cuando la información, aún siendo facilitada de forma disociada, contuviera elementos suficientes que pudieran permitir la identificación de los interesados en el proceso de reutilización, la prohibición de revertir el procedimiento de disociación mediante la adición de nuevos datos obtenidos de otras fuentes.

**Artículo 9.** *Licencias.*

1. Las Administraciones y organismos del sector público incluidos dentro del ámbito de aplicación de esta Ley, fomentarán el uso de licencias abiertas con las mínimas restricciones posibles sobre la reutilización de la información.

2. En los casos en los que se otorgue una licencia, ésta deberá reflejar, al menos, la información relativa a la finalidad concreta para la que se concede la reutilización, indicando igualmente si la misma podrá ser comercial o no comercial, para la que se concede la reutilización, la duración de la licencia, las obligaciones del beneficiario y del organismo concedente, las responsabilidades de uso y modalidades financieras, indicándose el carácter gratuito o, en su caso, la tarifa aplicable.

TÍTULO III

**Procedimiento y régimen sancionador**

**Artículo 10.** *Procedimiento de tramitación de solicitudes de reutilización.*

1. Las solicitudes de reutilización de documentos administrativos deberán dirigirse al órgano competente, entendiendo por tal aquel en cuyo poder obren los documentos cuya reutilización se solicita. Las solicitudes se presentarán por aquellas personas físicas o jurídicas que pretendan reutilizar los documentos de conformidad con lo previsto en esta Ley.

No obstante, cuando el órgano al que se ha dirigido la solicitud no posea la información requerida pero tenga conocimiento del sujeto previsto en el artículo 2 que la posee, le remitirá a la mayor brevedad posible la solicitud dando cuenta de ello al solicitante.

Cuando ello no sea posible, informará directamente al solicitante sobre el sujeto previsto en el artículo 2 al que, según su conocimiento, ha de dirigirse para solicitar dicha información.

2. La solicitud deberá reflejar el contenido previsto en el artículo 66.1 de la Ley 39/2015, de 1 de octubre, identificando el documento o documentos susceptibles de reutilización y especificando los fines, comerciales o no comerciales, de la reutilización. No obstante, cuando una solicitud esté formulada de manera imprecisa, el órgano competente pedirá al solicitante que la concrete y le indicará expresamente que si así no lo hiciera se le tendrá por desistido de su solicitud, en los términos previstos en el artículo 68 de la Ley 39/2015, de 1 de octubre. El solicitante deberá concretar su petición en el plazo de diez días a contar desde el día siguiente al de la recepción de dicho requerimiento. A estos efectos, el órgano competente asistirá al solicitante para delimitar el contenido de la información solicitada.

El cómputo del plazo para resolver la solicitud de información se entenderá suspendido por el tiempo que medie entre la notificación del requerimiento y su efectivo cumplimiento por el destinatario o, en su defecto, por el transcurso del plazo concedido, informándose al solicitante de la suspensión del plazo para resolver.

3. El órgano competente resolverá las solicitudes de reutilización en el plazo máximo de veinte días desde la recepción de la solicitud en el registro del órgano competente para su tramitación, con carácter general. Cuando por el volumen y la complejidad de la información solicitada resulte imposible cumplir el citado plazo se podrá ampliar el plazo de resolución en otros veinte días. En este caso deberá informarse al solicitante, en el plazo máximo de diez días, de toda ampliación del plazo, así como de las razones que lo justifican.

4. Las resoluciones que tengan carácter estimatorio podrán autorizar la reutilización de los documentos sin condiciones o bien supondrán el otorgamiento de la oportuna licencia para su reutilización en las condiciones pertinentes impuestas a través de la misma. En todo

caso la resolución estimatoria supondrá la puesta a disposición del documento en el mismo plazo previsto en el apartado anterior para resolver.

5. Si la resolución denegara total o parcialmente la reutilización solicitada, se notificará al solicitante, comunicándole los motivos de dicha negativa en los plazos mencionados en el apartado 3, motivos que habrán de estar fundados en alguna de las disposiciones de esta Ley o en el ordenamiento jurídico vigente.

6. En caso de que la resolución desestimatoria esté fundada en la existencia de derechos de propiedad intelectual o industrial por parte de terceros, el órgano competente deberá incluir una referencia a la persona física o jurídica titular de los derechos cuando ésta sea conocida, o, alternativamente, al cedente del que el organismo haya obtenido los documentos. Las bibliotecas, incluidas las universitarias, los museos y los archivos no estarán obligadas a incluir tal referencia.

7. En todo caso, las resoluciones adoptadas deberán contener una referencia a las vías de recurso a que pueda acogerse en su caso el solicitante, en los términos previstos en el artículo 40 de la Ley 39/2015, de 1 de octubre.

8. Si en el plazo máximo previsto para resolver y notificar no se hubiese dictado resolución expresa, el solicitante podrá entender desestimada su solicitud.

9. Las sociedades mercantiles públicas previstas en el párrafo c) del artículo 2, los centros de enseñanza, las organizaciones que realicen actividades de investigación o que financien tales actividades no estarán obligadas a cumplir lo previsto en este artículo.

**Artículo 10.bis.** *Unidad responsable de información.*

1. Cada sujeto previsto en el artículo 2 determinará la Unidad responsable de garantizar la puesta a disposición de su información.

2. En la Administración General del Estado se designarán las Unidades responsables de información en el ámbito de las Subsecretarías de cada Departamento. Los restantes sujetos previstos en el artículo 2 del sector público estatal con personalidad jurídica propia designarán sus Unidades correspondientes.

3. La Unidad responsable de información tendrá las siguientes funciones:

a) Coordinar las actividades de reutilización de la información con las políticas existentes en materia de publicaciones, información administrativa y administración electrónica.

b) Facilitar información sobre los órganos competentes, dentro de su ámbito, para la recepción, tramitación y resolución de las solicitudes de reutilización que se tramiten de acuerdo con lo previsto en el artículo 10.

c) Promover que la información sea provista en los formatos adecuados y esté actualizada en la medida de lo posible.

d) Coordinar y fomentar las actividades de promoción, concienciación y formación.

**Artículo 11.** *Régimen sancionador.*

1. En el ámbito de la Administración General del Estado, se considerarán infracciones muy graves a lo previsto en esta ley:

a) La desnaturalización del sentido de la información para cuya reutilización se haya concedido una licencia;

b) La alteración muy grave del contenido de la información para cuya reutilización se haya concedido una licencia.

2. Se considerarán infracciones graves:

a) La reutilización de documentación sin haber obtenido la correspondiente licencia en los casos en que ésta sea requerida;

b) La reutilización de la información para una finalidad distinta a la que se concedió;

c) La alteración grave del contenido de la información para cuya reutilización se haya concedido una licencia;

d) El incumplimiento grave de otras condiciones impuestas en la correspondiente licencia o en la normativa reguladora aplicable.

3. Se considerarán infracciones leves:

a) La falta de mención de la fecha de la última actualización de la información;
b) La alteración leve del contenido de la información para cuya reutilización se haya concedido una licencia;
c) La ausencia de cita de la fuente de acuerdo con lo previsto en el artículo 8 de esta ley;
d) El incumplimiento leve de otras condiciones impuestas en la correspondiente licencia o en la normativa reguladora aplicable.

4. Por la comisión de las infracciones recogidas en este artículo, se impondrán las siguientes sanciones:

a) Sanción de multa de 50.001 a 100.000 euros por la comisión de infracciones muy graves;
b) Sanción de multa de 10.001 a 50.000 euros por la comisión de infracciones graves;
c) Sanción de multa de 1.000 a 10.000 euros. Por la comisión de infracciones leves.

Por la comisión de infracciones muy graves y graves recogidas, además de las sanciones previstas en las letras a) y b), se podrá sancionar con la prohibición de reutilizar documentos sometidos a licencia durante un periodo de tiempo entre 1 y 5 años y con la revocación de la licencia concedida.
5. Las sanciones se graduarán atendiendo a la naturaleza de la información reutilizada, al volumen de dicha información, a los beneficios obtenidos, al grado de intencionalidad, a los daños y perjuicios causados, en particular a los que se refieren a la protección de datos de carácter personal, a la reincidencia y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.
6. La potestad sancionadora se ejercerá, en todo lo no previsto en la presente ley, de conformidad con lo dispuesto en el Capítulo III de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Su ejercicio corresponderá a los órganos competentes que la tengan atribuida por razón de la materia.
7. El régimen sancionador previsto en esta ley se entiende sin perjuicio de la responsabilidad civil o penal en que pudiera incurrirse, que se hará efectiva de acuerdo con las correspondientes normas legales.

**Disposición adicional primera.** *Planes y programas.*

El Gobierno, a propuesta de los Ministerios competentes, desarrollará planes y programas de actuaciones dirigidos a facilitar la reutilización de la información del sector público en aras de promover el crecimiento del sector de contenidos digitales, pudiendo establecer con el resto de las Administraciones públicas los mecanismos de colaboración que se estimen pertinentes para la consecución de dicho objetivo.

**Disposición adicional segunda.** *Aplicación a otros organismos.*

1. Lo previsto en esta ley será de aplicación a los documentos conservados por organismos e instituciones diferentes a los mencionados en el artículo 2, a los que, en los términos previstos en su normativa reguladora, resulte aplicable en su actividad la Ley 39/2015, de 1 de octubre.
2. Las previsiones contenidas en la presente ley serán de aplicación a las sentencias y resoluciones judiciales, sin perjuicio de lo previsto en el artículo 107.10 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y su desarrollo específico.

**Disposición adicional tercera.** *Transferencia para Reutilización Pública de Microdatos de Encuestas correspondientes a Investigaciones Sociológicas.*

1. Los proyectos de investigación, análisis, o diagnóstico social que vayan a ser desarrollados por los sujetos relacionados en el artículo 2.a), b), c) y d) siempre que impliquen la realización de encuestas cuantitativas en el ámbito de las ciencias sociales con toma de datos, deberán incorporar en su diseño un plan para la inclusión de la documentación y microdatos anonimizados de dicha encuesta en un Banco de Datos específico, creado en el Centro de Investigaciones Sociológicas. Este Plan se depositará en el mencionado Banco de Datos en los 12 meses posteriores a la aprobación del proyecto, y

los microdatos anonimizados que integren el estudio deberán transferirse en un periodo no superior a cuatro años desde la aprobación del proyecto. Este plazo podrá ser ampliado excepcionalmente por causas derivadas del desarrollo y conclusión del proyecto.

2. No obstante lo dispuesto en el apartado anterior, quedan excluidas de tal obligación:

a) Las encuestas realizadas por Agencias Estatales, las entidades públicas empresariales, las sociedades mercantiles estatales, las fundaciones públicas y las entidades de Derecho Público con independencia funcional o con una especial autonomía reconocida por la Ley cuando actúen en régimen de derecho privado.

b) Las realizadas por la Sociedad Estatal de Participaciones Industriales, o cualquiera de las empresas o fundaciones de su Grupo, el Instituto Nacional de Estadística (INE) y los organismos similares de las Comunidades Autónomas.

c) Las encuestas que conformen las estadísticas de carácter oficial incluidas en los correspondientes Planes Estadísticos Nacionales y sujetas a la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, así como las estadísticas europeas sujetas a su normativa específica. No obstante, en este caso, el INE impulsará, como coordinador del Sistema Estadístico de la Administración del Estado, que se dé la publicidad debida a los microdatos de estas encuestas con finalidad estadística elaboradas por estos organismos.

3. No serán objeto de transferencia los microdatos obtenidos de registros administrativos de datos, así como los utilizados para las encuestas que sean determinantes o indispensables para la política estratégica interna de las entidades que las lleven a cabo en los términos que se determine reglamentariamente.

4. Las empresas, equipos de investigación particulares y personas físicas o jurídicas que realicen asimismo este tipo de proyectos a través encuestas cuantitativas en el ámbito de las ciencias sociales con toma de datos, y que reciban ayudas o subvenciones públicas, siempre que las mismas supongan más del 50% de los fondos con que se financien sus proyectos de investigación, estarán igualmente sometidas a la presentación del plan y a la obligación de transferir los datos para la obtención de la misma. En la normativa reguladora del régimen subvencional de ayudas públicas para este tipo de proyectos y en sus sucesivas convocatorias, especialmente aquellas derivadas del Plan Nacional de I+D+i y el Plan Nacional de la Ciencia, se harán constar estas obligaciones. No obstante, respecto de estos sujetos será aplicable la misma posibilidad de exclusión cuando la publicación de los microdatos pudiera causar un perjuicio competitivo irreparable en su posicionamiento empresarial en el mercado.

5. El incumplimiento de esta obligación por parte de los equipos investigadores responsables, especialmente en el marco de los Planes Nacionales de Investigación Científica, Desarrollo e Innovación Tecnológica, supondrá causa de exclusión a la hora de solicitar nuevas ayudas de financiación pública, de acuerdo con los procedimientos sancionadores previstos en la Ley 38/2003, de 17 de noviembre, General de Subvenciones.

**Disposición adicional cuarta.** *Reutilización de documentos, archivos y colecciones de origen privado.*

En cuanto a los documentos, archivos y colecciones de origen privado, conservadas en los archivos, bibliotecas (incluidas las universitarias) y museos, su puesta a disposición con fines de reutilización, ha de respetar las condiciones establecidas en el instrumento jurídico correspondiente que haya dado lugar a la conservación y custodia de estos fondos en instituciones culturales públicas.

**Disposición adicional quinta.** *Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).*

Con relación a la reutilización de determinadas categorías de datos protegidos a que se refiere el capítulo II del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) que obren en poder de los sujetos previstos en los párrafos a) y b) de esta ley, sin perjuicio de la aplicación

directa de los preceptos de dicho Reglamento, se aplicarán asimismo las siguientes previsiones:

a) El régimen sancionador previsto en el artículo 11 de esta ley, en el ámbito de la Administración General del Estado, y a tal efecto:

1.º Se considerará infracción muy grave de las previstas en el artículo 11.1 el incumplimiento de las condiciones de acceso a los datos protegidos o de las condiciones impuestas para preservar la seguridad e integridad del entorno de tratamiento seguro utilizado.

2.º Se considerarán infracciones graves de las previstas en el artículo 11.2, las siguientes:

i. El incumplimiento por el reutilizador de su compromiso formal de confidencialidad que prohíba la divulgación de la información contenida en las categorías de datos protegidos.

ii. La reidentificación por el reutilizador de los interesados a quienes se refieran los datos protegidos.

iii. La falta de notificación de los incidentes de seguridad o cualquier otra violación de la seguridad de los datos protegidos reutilizados que den lugar o conlleven riesgo de reidentificación de los interesados.

b) Los sujetos previstos en los párrafos a) y b) del artículo 2 que permitan la reutilización de las categorías de datos protegidos podrán exigir el pago de una tasa por la misma, que se calculará en función de los costes relacionados con la tramitación de las solicitudes de reutilización de las categorías de datos enumeradas en el artículo 3.1 del Reglamento y se limitará a los costes necesarios en relación con:

i. La reproducción, la entrega y la difusión de los datos;

ii. La adquisición de derechos;

iii. La anonimización u otras formas de preparación de los datos personales y de los datos comerciales confidenciales con arreglo a lo dispuesto en el artículo 5.3 del Reglamento;

iv. El mantenimiento del entorno de tratamiento seguro;

v. La adquisición, por parte de terceros ajenos al sector público, del derecho de terceros de permitir la reutilización de conformidad con el capítulo II del Reglamento, y

vi. La asistencia a los reutilizadores en la obtención del consentimiento de los interesados y del permiso de los titulares de datos cuyos derechos e intereses puedan verse afectados por la reutilización.

El establecimiento y la regulación de los elementos esenciales de dicha tasa deberá ajustarse a lo previsto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos y demás normativa tributaria aplicable. En todo caso deberá ser transparente, no discriminatoria y proporcionada, estar justificada objetivamente y respetar las restantes condiciones contempladas en el artículo 6 del Reglamento.

c) Con relación al procedimiento de tramitación de solicitudes de datos protegidos se aplicará lo dispuesto en el artículo 5 del Reglamento y el artículo 10 de la ley, con las siguientes especialidades:

i. El plazo para resolver el procedimiento será de dos meses a contar desde la recepción de la solicitud por el órgano competente.

ii. Cuando la solicitud sea excepcionalmente extensa o compleja, el órgano competente para dictar resolución podrá ampliar el plazo para resolver hasta un máximo de 30 días previa notificación al interesado en los términos previstos en el artículo 32 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las administraciones públicas.

Contra la resolución que se dicte concediendo o denegando la reutilización, el interesado podrá interponer los recursos que procedan en vía administrativa y jurisdiccional, de conformidad con lo establecido en la Ley 39/2015, de 1 de octubre, y en la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Si en el plazo máximo previsto para resolver y notificar no se hubiese dictado resolución expresa, el solicitante podrá entender desestimada su solicitud.

Los sujetos previstos en los párrafos a) y b) del artículo 2 comunicarán al Ministerio de Asuntos Económicos y Transformación Digital la identidad de los organismos competentes para prestar asistencia designados, en su caso, en virtud del artículo 5.1 del Reglamento, con objeto de dar cumplimiento a las previsiones de notificación a la Comisión previstas en el artículo 7.5 del mismo. Asimismo, comunicarán toda modificación posterior de la identidad de dichos organismos competentes.

**Disposición transitoria única.** *Régimen transitorio aplicable a los acuerdos exclusivos.*

Los acuerdos exclusivos existentes a 17 de julio de 2013 a los que no se aplique la excepción contemplada en los apartados 2 y 3 del artículo 6 y que fuesen celebrados por los sujetos previstos en los párrafos a) y b) del artículo 2 concluirán cuando expire el contrato o, en cualquier caso, no más tarde del 18 de julio de 2043.

Sin perjuicio de lo previsto en el párrafo anterior, los acuerdos exclusivos existentes a 16 de julio de 2019 a los que no se apliquen las excepciones contempladas en los apartados 2 y 3 del artículo 6 que fuesen celebrados por los sujetos previstos en el párrafo c) del artículo 2, concluirán cuando expire el contrato o, en cualquier caso, no más tarde del 17 de julio de 2049.

**Disposición final primera.** *Fundamento constitucional.*

La presente ley tiene carácter de legislación básica al amparo de lo dispuesto en el artículo 149.1.18 ª de la Constitución Española. Se exceptúan los apartados 1 (párrafos segundo y tercero), 3 y 8 del artículo 10, el apartado 2 del artículo 10.bis. y el artículo 11.

**Disposición final segunda.** *Desarrollo reglamentario.*

El Gobierno, en el ámbito de sus competencias, dictará cuantas disposiciones sean necesarias para la ejecución y desarrollo de lo establecido en esta ley.

**Disposición final tercera.** *Entrada en vigor.*

Esta Ley entrará en vigor a los dos meses de su publicación en el «Boletín Oficial del Estado».

**Anexo**

**Definiciones**

A efectos de la presente Ley, se entiende por:

1) Anonimización: Proceso por el que se transforman documentos en documentos anónimos que no se refiere a una persona física identificada o identificable o al proceso de convertir datos personales que se hayan anonimizado, de forma que el interesado no sea identificable o haya dejado de serlo.

2) Conjuntos de datos de alto valor: Documentos cuya reutilización está asociada a considerables beneficios para la sociedad, el medio ambiente y la economía, en particular debido a su idoneidad para la creación de servicios de valor añadido, aplicaciones y puestos de trabajo nuevos, dignos y de calidad, y del número de beneficiarios potenciales de los servicios de valor añadido y aplicaciones basados en tales conjuntos de datos.

3) Datos abiertos: Son aquellos que cualquiera es libre de utilizar, reutilizar y redistribuir, con el único límite, en su caso, del requisito de atribución de su fuente o reconocimiento de su autoría.

4) Datos dinámicos: Documentos en formato digital, sujetos a actualizaciones frecuentes o en tiempo real, debido, en particular, a su volatilidad o rápida obsolescencia; los datos generados por los sensores suelen considerarse datos dinámicos.

5) Datos de investigación: Documentos en formato digital, distintos de las publicaciones científicas, recopilados o elaborados en el transcurso de actividades de investigación científica y utilizados como prueba en el proceso de investigación, o comúnmente aceptados

en la comunidad investigadora como necesarios para validar las conclusiones y los resultados de la investigación.

6) Documento: Toda información o parte de ella, cualquiera que sea su soporte o forma de expresión, sea esta textual, gráfica, sonora visual o audiovisual, incluyendo los metadatos asociados y los datos contenidos con los niveles más elevados de precisión y desagregación. A estos efectos no se considerarán documentos los programas informáticos que estén protegidos por la legislación específica aplicable a los mismos.

7) Formato legible por máquina: Un formato de archivo estructurado que permita a las aplicaciones informáticas identificar, reconocer y extraer con facilidad datos específicos, incluidas las declaraciones fácticas y su estructura interna.

8) Formato abierto: Un formato de archivo independiente de plataformas y puesto a disposición del público sin restricciones que impidan la reutilización de los documentos.

9) Licencia tipo: Conjunto de condiciones de reutilización predefinidas en formato digital, preferiblemente compatibles con licencias modelo públicas disponibles en línea.

10) Norma formal abierta: Una norma establecida por escrito que especifica los criterios de interoperabilidad de la aplicación informática.

11) Tercero: Toda persona física o jurídica distinta de un sujeto previsto en el artículo 2 que esté en posesión de los datos.

12) Universidad: Todo organismo del sector público que imparta enseñanza superior post-secundaria conducente a la obtención de títulos académicos.

## § 5

# Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal

Ministerio de la Presidencia
«BOE» núm. 269, de 8 de noviembre de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-17560

La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, por medio de la cual se incorpora a nuestro ordenamiento jurídico la Directiva 2003/98/CE, de 17 de noviembre de 2003, del Parlamento Europeo y del Consejo, relativa a la reutilización de la información del sector público, establece el régimen jurídico general para la reutilización de dicha información.

La citada ley reconoce la importancia y el valor que tiene la información generada desde las instancias públicas por el interés que posee para las empresas y, consecuentemente, para el crecimiento económico y la creación de empleo. Asimismo, señala el interés de la citada información para los ciudadanos y ciudadanas, como elemento de apertura y participación democrática.

La Ley 37/2007, de 16 de noviembre, no modifica el régimen de acceso a los documentos administrativos consagrado en nuestro ordenamiento jurídico, sino que aporta un valor añadido al derecho de acceso, contemplando el régimen normativo básico para el uso por parte de terceros de la información que obra en poder del sector público, con fines comerciales o no comerciales, en un marco de libre competencia, regulando las condiciones mínimas a las que debe acogerse un segundo nivel de tratamiento de la información. En este sentido, la Ley 37/2007, de 16 de noviembre, establece las bases para promover la reutilización de la información pública y garantiza que ésta se lleve a cabo en el marco de unas condiciones claras, transparentes y no discriminatorias.

Por otra parte, favorecer la reutilización de la información pública figura entre los objetivos políticos establecidos para la Administración Electrónica en la Declaración Ministerial de Malmö, de noviembre de 2009, que fija las prioridades de la Unión Europea dentro de este ámbito para el periodo 2010-2015, y han sido desarrolladas en el Plan de Acción de la Unión Europea sobre Administración Electrónica en el período 2011-2015. Este objetivo se ha visto consolidado en la Declaración Ministerial de Granada, de abril de 2010, y en la nueva Agenda Digital Europea, de mayo de 2010, que guiará el futuro de la Unión Europea en materia de sociedad de la información hasta el año 2015.

El presente real decreto se enmarca en el conjunto de medidas que constituyen la Estrategia 2011-2015 del Plan Avanza 2, que prevé entre sus medidas normativas el desarrollo reglamentario de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, al objeto de detallar para el ámbito del sector público estatal

las disposiciones de esta Ley, promoviendo y facilitando al máximo la puesta a disposición de la información del sector público.

El capítulo I del real decreto establece en el artículo 1 su objeto y ámbito de aplicación, manteniendo el ámbito de aplicación objetiva de la Ley 37/2007, de 16 de noviembre, y acotando su ámbito de aplicación subjetiva al sector público estatal.

El capítulo II del real decreto contiene el régimen jurídico de la reutilización de la información del sector público estatal. Así, el artículo 2 establece el principio general de que, en el ámbito del sector público estatal, estará autorizada la reutilización de los documentos elaborados o custodiados por las personas jurídico-públicas que lo forman, sin perjuicio del régimen aplicable al derecho de acceso a los documentos establecido en el artículo 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y de las demás normas que regulan el derecho de acceso o la publicidad registral con carácter específico.

El artículo 3 del real decreto tiene por objeto regular determinadas responsabilidades y funciones en materia de reutilización en cada departamento ministerial, organismo o entidad del sector público.

El artículo 4 del real decreto supone un desarrollo de lo dispuesto en el apartado 5 del artículo 4 de la Ley 37/2007, de 16 de noviembre. En este artículo se establece que las entidades del sector público estatal informarán, a través de su sede electrónica, sobre los documentos reutilizables elaborados o custodiados por ellas. La publicación de la información sobre los documentos reutilizables en la sede electrónica, prevista en el artículo 4 no implica necesariamente que los propios documentos reutilizables se pongan a disposición del público a través de la sede electrónica, siendo posible que dicha puesta a disposición se realice a través de páginas de Internet u otros medios electrónicos.

El artículo 5 prevé el mantenimiento de un catálogo de información pública reutilizable correspondiente, al menos, a la Administración General del Estado y demás organismos y entidades que forman parte del sector público estatal, que permitirá acceder desde un único punto a los recursos de información pública reutilizable existentes.

El artículo 6 establece determinados mecanismos de coordinación pertinentes en el ámbito del sector público estatal, en particular, en lo que se refiere a la puesta a disposición de información reutilizable por medios electrónicos.

El capítulo III desarrolla el régimen de modalidades de reutilización de los documentos reutilizables establecido en la Ley 37/2007, de 16 de noviembre, promoviendo al máximo la homogeneidad, claridad y sencillez del régimen de condiciones aplicables a la reutilización, contribuyendo de este modo al mayor aprovechamiento de las posibilidades de reutilización y a impulsar la competencia y la innovación.

El artículo 7 establece ciertas condiciones generales para la reutilización de la información, exigibles en todo caso, que constituyen un desarrollo de los contenidos potestativos establecidos en el artículo 8 de la Ley 37/2007, de 16 de noviembre. Entre otras condiciones, se prohíbe que el sentido de la información sea desnaturalizado, es decir, que sea tergiversado o falseado.

El apartado 1 del artículo 8 establece que, en el ámbito subjetivo de aplicación del real decreto, la modalidad general de puesta a disposición de los documentos reutilizables será la puesta a disposición para la reutilización sin sujeción a condiciones específicas, siendo únicamente aplicables las condiciones generales antes mencionadas. De este modo, el real decreto establece como regla general de aplicación la modalidad más favorable a la reutilización, que deberá ser la que se siga en la generalidad de los casos. No obstante, para los supuestos en los que la modalidad general de puesta a disposición no resulte adecuada, se puede considerar el establecimiento de condiciones específicas adicionales a las condiciones generales previstas en este artículo. En tales supuestos, se podrá optar por aplicar alguna de las otras modalidades de puesta a disposición establecidas en la Ley 37/2007, de 16 de noviembre, en los términos desarrollados por los apartados 2 a 4 del artículo 8 del real decreto. Asimismo, se prevé que la puesta a disposición a través del procedimiento de solicitud previa establecido en el artículo 10 de la Ley 37/2007, de 16 de noviembre, sólo sea empleado cuando la naturaleza de los documentos así lo exija, por ejemplo, cuando correspondan a documentos que no preexistan en formato electrónico y en otros casos excepcionales debidamente motivados.

El capítulo IV regula el régimen aplicable a los documentos reutilizables sujetos a derechos de propiedad intelectual o que contengan datos personales.

Conforme a lo establecido en el artículo 3.3 de la Ley 37/2007, de 16 de noviembre, el artículo 9 prevé que la reutilización de los documentos sobre los que existan derechos de propiedad intelectual o industrial de terceros sólo podrá ser autorizada si se dispone de la preceptiva y suficiente cesión de los derechos de explotación por parte de las personas titulares de los mismos.

Por su parte, el artículo 10 desarrolla el mandato establecido en el artículo 3.3.e), de la Ley 37/2007, de 16 de noviembre, de que el ejercicio de los derechos de propiedad intelectual de las Administraciones y organismos del sector público sobre sus documentos deberá realizarse de forma que se facilite su reutilización, previendo que la puesta a disposición de los documentos para su reutilización conllevará la cesión no exclusiva de los derechos de propiedad intelectual correspondientes.

Finalmente, el artículo 11 establece, en relación con los documentos que contengan datos de carácter personal, que podrá procederse a autorizar su reutilización siempre y cuando se proceda previamente a un proceso de disociación, de conformidad con lo establecido en la normativa de protección de datos de carácter personal.

Conforme a lo dispuesto por el artículo 14.11 de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, el uso del masculino genérico en el texto de esta disposición debe considerarse como inclusivo de ambos géneros.

El presente real decreto se dicta en virtud de la habilitación contenida en la disposición final segunda de la Ley 37/2007, de 16 de noviembre y ha sido informado por el Consejo Superior de Administración Electrónica y el Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información y sometido a consulta pública.

En su virtud, a propuesta del Ministro de Industria, Turismo y Comercio, y del Vicepresidente del Gobierno de Política Territorial y Ministro de Política Territorial y Administración Pública, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 21 de octubre de 2011,

DISPONGO:

CAPÍTULO I

**Disposiciones generales**

**Artículo 1.** *Objeto y ámbito de aplicación.*

1. El presente real decreto tiene por objeto desarrollar la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, en el ámbito del sector público estatal, en lo relativo al régimen jurídico de la reutilización, las obligaciones del sector público estatal, las modalidades de reutilización de los documentos reutilizables y el régimen aplicable a documentos reutilizables sujetos a derechos de propiedad intelectual o que contengan datos personales.

2. Se entiende que forman parte del sector público estatal, a los efectos de esta norma, los siguientes entes, organismos y entidades:

a) La Administración General del Estado.

b) Las entidades gestoras y los servicios comunes de la Seguridad Social.

c) Los organismos autónomos y las agencias estatales dependientes de la Administración General del Estado.

d) Las entidades de derecho público dependientes de la Administración General del Estado o vinculadas a ella, que cumplan los requisitos del artículo 2.d) de la Ley 37/2007, de 16 de noviembre.

e) Las entidades estatales de derecho público distintas a las mencionadas en los párrafos c) y d) de este apartado y que, con independencia funcional o con una especial autonomía reconocida por ley, tengan atribuidas funciones de regulación o control de carácter externo sobre un determinado sector o actividad.

f) Las fundaciones del sector público estatal, definidas en el artículo 44 de la Ley 50/2002, de 26 de diciembre, de Fundaciones.

g) Los consorcios, formados por entes, entidades u organismos del sector público estatal, dotados de personalidad jurídica propia.

h) Las asociaciones constituidas por las Administraciones, organismos y entidades mencionados en los párrafos anteriores de este apartado.

3. El presente real decreto se aplicará a los documentos elaborados o custodiados por el sector público estatal cuya reutilización esté autorizada conforme a la Ley 37/2007, de 16 de noviembre y a esta norma y que no se encuentren recogidos en las excepciones previstas en el artículo 3 de la misma Ley.

4. Lo previsto en este real decreto no restringirá las previsiones más favorables que, sobre acceso o reutilización de la información, se establezcan en las disposiciones sectoriales específicas.

5. A los efectos de esta norma se entiende por «agente reutilizador» toda persona, física o jurídica que reutilice información del sector público, ya sea para fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública.

## CAPÍTULO II

## Régimen jurídico y organizativo de la reutilización de la información en el sector público estatal

**Artículo 2.** *Autorización general para la reutilización de los documentos del sector público y puesta a disposición por medios electrónicos.*

1. Los órganos de la Administración General del Estado y los demás organismos y entidades a que se hace referencia en el artículo 1.2 autorizarán la reutilización de los documentos elaborados o custodiados por ellos e incluidos en el ámbito de aplicación de este real decreto, sin perjuicio de lo dispuesto en el régimen aplicable al derecho de acceso a los documentos en virtud de lo previsto en el artículo 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y las demás normas que regulan el derecho de acceso, la reutilización de la información del sector público o la publicidad registral con carácter específico. Únicamente podrá denegarse motivadamente la reutilización de los documentos si concurre alguno de los supuestos establecidos en el apartado 3 del artículo 3 de la Ley 37/2007, de 16 de noviembre.

2. Se pondrán a disposición del público los documentos reutilizables que se encuentren previamente disponibles en formato electrónico por medios electrónicos, de una manera estructurada y usable para los interesados e interesadas y preferentemente en bruto, en formatos procesables y accesibles de modo automatizado correspondientes a estándares abiertos en los términos establecidos en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. Asimismo, los documentos reutilizables y los medios electrónicos de puesta a disposición de los mismos deberán ser accesibles a las personas con discapacidad de acuerdo con la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y su normativa de desarrollo aplicable.

3. Se procurará que la información puesta a disposición se actualice en un tiempo razonable que permita el uso adecuado de dicha información, con una frecuencia análoga con la que actualicen dicha información internamente, así como su disponibilidad, incluida la temporal, completitud e integridad de acuerdo con el marco normativo aplicable en cada caso.

4. Los documentos en formato electrónico reutilizables podrán incluir entre sus metadatos una indicación de su última fecha de actualización y una referencia a las condiciones de reutilización aplicables en cada momento conforme a lo dispuesto en los artículos 7 y 8, en los términos que se establezcan conforme al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

5. Los documentos reutilizables en formato no electrónico serán puestos a disposición del público previa solicitud, en los términos establecidos en el artículo 8.4.

**Artículo 3.** *Coordinación en materia de reutilización de los órganos, organismos y entidades del sector público estatal.*

1. Los órganos de la Administración General del Estado y los demás organismos y entidades a que se hace referencia en el artículo 1.2 contarán con un órgano encargado de la coordinación de las actividades de reutilización de la información.

En los departamentos ministeriales esta labor de coordinación recaerá en la persona titular de la Subsecretaría del departamento y en los organismos vinculados o dependientes en la persona titular de éstos, sin perjuicio de las atribuciones competenciales que establezcan normas sectoriales específicas y sin perjuicio de las responsabilidades que corresponden a los órganos que deban autorizar la reutilización de la información en cada caso.

En el ejercicio de esa labor de coordinación, corresponderá a dichos órganos:

a) Coordinar las actividades de reutilización de la información con las políticas del departamento u organismo relativas a las publicaciones, la información administrativa y la administración electrónica, así como coordinar la remisión de información sobre las actividades realizadas en materia de reutilización dentro de su ámbito a la Secretaría de Estado para la Función Pública del Ministerio de Política Territorial y Administración Pública, que la trasladará al Consejo Superior de Administración Electrónica.

b) Facilitar información sobre los órganos competentes dentro de su ámbito para la recepción, tramitación y resolución de las solicitudes de reutilización que se tramiten de acuerdo con el artículo 10 de la Ley 37/2007, de 16 de noviembre, así como coordinar la provisión de la información sobre los documentos reutilizables prevista en el artículo 4.

c) Resolver, cuando proceda, las quejas y sugerencias que se presenten en materia de reutilización de la información, conforme al Real Decreto 951/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

Los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 facilitarán a los correspondientes servicios de información de los Departamentos ministeriales o de dichos organismos y entidades los datos de contacto de aquellos que deban autorizar la reutilización de los documentos elaborados o custodiados por ellos, a efectos de que dichos servicios de información faciliten dichos datos de contacto al público, al menos, por medios electrónicos.

2. Los órganos de la Administración General del Estado y los demás organismos y entidades a que se hace referencia en el artículo 1.2 no serán responsables del uso que de su información hagan los agentes reutilizadores.

3. El ejercicio de la potestad sancionadora, con sujeción a lo establecido en el artículo 11 de la Ley 37/2007, de 16 de noviembre, corresponderá, en el caso de infracciones muy graves, a las personas titulares del departamento ministerial, y en el caso de infracciones graves o leves a los órganos titulares de la información pública correspondiente con rango mínimo de Dirección General. En el caso de los demás organismos mencionados en el artículo 1.2, la competencia corresponderá en todos los casos a la persona titular del organismo, ente o entidad de que se trate.

**Artículo 4.** *Información sobre los documentos susceptibles de reutilización.*

1. Los órganos de la Administración General del Estado y los demás organismos y entidades a que se hace referencia en el artículo 1.2 informarán de manera estructurada y usable, preferentemente a través de un espacio dedicado de su sede electrónica con la ubicación «sede.gob.es/datosabiertos», sobre qué documentación es susceptible de ser reutilizada, los formatos en que se encuentra disponible, las condiciones aplicables a su reutilización, indicando la fecha de la última actualización de los documentos reutilizables, proporcionando, cuando esté disponible, la información complementaria precisa para su comprensión y procesamiento automatizado y facilitando al máximo la identificación,

búsqueda y recuperación de los documentos disponibles para su reutilización mediante mecanismos tales como listados, bases de datos o índices de información reutilizable.

Igualmente, se informará, preferentemente a través de la correspondiente sede electrónica, sobre la modalidad o, en su caso, modalidades de puesta a disposición de los documentos reutilizables que sean de aplicación conforme a los artículos 7 y 8.

Se procurará que la información sobre los documentos reutilizables prevista en este apartado sea procesable y accesible de modo automatizado.

2. En caso de que apliquen tasas o precios públicos a la reutilización de sus documentos se publicará, preferentemente en la sede electrónica correspondiente, el listado de tasas y precios públicos que sean de aplicación, así como la base de cálculo utilizada para la determinación de los mismos, conforme a lo dispuesto en el artículo 7 de la Ley 37/2007, de 16 de noviembre.

**Artículo 5.** *Catálogo de Información Pública reutilizable.*

1. La Secretaría de Estado para la Función Pública del Ministerio de Política Territorial y Administración Pública y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio mantendrán un catálogo de información pública reutilizable correspondiente, al menos, a la Administración General del Estado y a los demás organismos y entidades a que se refiere el artículo 1.2, que permita acceder, desde un único punto, a los distintos recursos de información pública reutilizable disponibles.

2. Este catálogo será accesible, al menos, desde el punto de acceso general previsto en el artículo 8 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y podrá enlazar e interoperar con iniciativas similares de la propia Administración General del Estado o de otras Administraciones Públicas en las condiciones que se convengan por ambas partes y en el marco de lo previsto en el presente real decreto.

3. Los órganos de la Administración General del Estado y los restantes organismos y entidades enumerados en el artículo 1.2 colaborarán con los departamentos ministeriales mencionados en el apartado 1 para la confección y el mantenimiento de dicho catálogo y asimismo serán responsables de la actualización constante de la información sobre los documentos reutilizables correspondiente a los mismos contenida en el citado catálogo, asegurando la plena coherencia del mismo con la información facilitada conforme al apartado 1 del artículo 4 de este real decreto.

**Artículo 6.** *Coordinación en materia de reutilización de la información del sector público en el ámbito de la Administración General del Estado.*

1. El Consejo Superior de Administración Electrónica, sin perjuicio de las competencias asignadas a otros órganos, coordinará los aspectos técnicos, necesarios para la aplicación de lo dispuesto en esta norma, relacionados con la reutilización de la información por medios electrónicos.

El Consejo Superior de Administración Electrónica elaborará y publicará durante el tercer trimestre de cada año un informe anual sobre las actividades en materia de reutilización de la información pública por medios electrónicos, tomando en consideración la información que le sea facilitada conforme al párrafo a) del apartado 1 del artículo 3.

2. La Secretaría de Estado para la Función Pública del Ministerio de Política Territorial y Administración Pública y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio ejercerán una función general de promoción de la reutilización de la información del sector público estatal, desarrollando, a tal efecto, actuaciones de información, asesoramiento general y soporte, sensibilización, formación y estudio en materia de reutilización, incluyendo, en su caso, el uso de redes sociales para la construcción de comunidades virtuales de administraciones, ciudadanos y ciudadanas y empresas con interés en la reutilización de la información pública.

3. Sin perjuicio de las competencias atribuidas a otros órganos, el Consejo Superior de Administración Electrónica evaluará periódicamente los aspectos técnicos de los servicios públicos relacionados con la reutilización de la información del sector público, y podrá dirigirse, de oficio o a instancia de parte, a otros órganos de la Administración General del

Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2, para la obtención de información y, en su caso, para la búsqueda de soluciones consensuadas en casos de supuestos de información pública cuya reutilización esté sujeta a restricciones de índole técnica.

CAPÍTULO III

**Modalidades de reutilización de los documentos reutilizables**

**Artículo 7.** *Condiciones generales de puesta a disposición de los documentos reutilizables.*

Serán de aplicación las siguientes condiciones generales para todas las modalidades de puesta a disposición de los documentos reutilizables:

a) No desnaturalizar el sentido de la información.
b) Citar la fuente de los documentos objeto de la reutilización.
c) Mencionar la fecha de la última actualización de los documentos objeto de la reutilización, siempre cuando estuviera incluida en el documento original.
d) No se podrá indicar, insinuar o sugerir que los órganos administrativos, organismos o entidades del sector público estatal titulares de la información reutilizada participan, patrocinan o apoyan la reutilización que se lleve a cabo con ella.
e) Conservar y no alterar ni suprimir los metadatos sobre la fecha de actualización y las condiciones de reutilización aplicables incluidos, en su caso, en el documento puesto a disposición para su reutilización por la Administración u organismo del sector público.

Estas condiciones generales serán accesibles mediante un aviso legal por medios electrónicos, de forma permanente, fácil y directa, preferentemente dentro de la ubicación «sede.gob.es/datosabiertos» de la sede electrónica del órgano de la Administración General del Estado, organismo o entidad correspondiente, y vincularán a cualquier agente reutilizador por el mero hecho de hacer uso de los documentos sometidos a ellas.
Dicho aviso legal incluirá el texto contenido en el anexo del presente real decreto.

**Artículo 8.** *Modalidades de puesta a disposición de los documentos reutilizables.*

1. La modalidad general básica para la puesta a disposición de los documentos reutilizables a que se refiere este real decreto será la puesta a disposición sin sujeción a condiciones específicas, prevista en el párrafo a) del apartado 2 del artículo 4 de la Ley 37/2007, de 16 de noviembre, aplicándose únicamente las condiciones generales establecidas en el artículo 7.
2. No obstante lo dispuesto en el apartado anterior, los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2, podrán optar de manera motivada por aplicar las modalidades previstas en los párrafos b) y c) del apartado 2 del artículo 4 de la Ley 37/2007, de 16 de noviembre, a la reutilización de determinados documentos que obren en su poder en los términos que se establecen en los siguientes apartados de este artículo.
A tal efecto, previamente y mediante orden ministerial o resolución del presidente del organismo correspondiente, salvo que por norma legal dicha competencia se atribuya específicamente a un órgano diferente, se determinará el régimen concreto de puesta a disposición aplicable, los documentos reutilizables sometidos al mismo y las condiciones específicas aplicables dentro del marco de lo dispuesto en la Ley 37/2007, de 16 de noviembre y las disposiciones de este real decreto. Las condiciones específicas deberán respetar, en todo caso, los criterios establecidos en el apartado 3 del artículo 4 de la misma Ley y deberán incluir, asimismo, los contenidos mínimos previstos en el artículo 9 de la misma.
3. La modalidad de puesta a disposición conforme al párrafo b) del apartado 2 del artículo 4 de la Ley 37/2007, de 16 de noviembre, se realizará con sujeción a condiciones específicas establecidas en licencias-tipo disponibles en formato digital y procesables electrónicamente. A tal efecto, los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 podrán emplear licencias-tipo existentes, denominadas «libres» siempre que se ajusten a lo

establecido en este real decreto y demás normativa aplicable, o proceder a establecer licencias-tipo específicas.

En todo caso, las condiciones específicas establecidas en dichas licencias-tipo para cada tipo de información pública reutilizable serán accesibles por medios electrónicos, de forma permanente, fácil y directa, preferentemente en la sede electrónica del órgano de la Administración General del Estado, organismo o entidad correspondiente de las enumerados en el artículo 1.2, de manera que puedan ser descargadas, almacenadas y reproducidas por los agentes reutilizadores, vinculándoles por el mero hecho de hacer uso de los documentos sometidos a ellas.

Asimismo, los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 facilitarán información al público por medios electrónicos sobre las licencias-tipo empleadas por el mismo a lo largo del tiempo y las condiciones específicas aplicables en cada momento, incluyendo expresamente información sobre su período de vigencia y posibles modificaciones de las condiciones específicas aplicables a la reutilización de cada tipo de información pública reutilizable.

Los agentes reutilizadores interesados podrán solicitar a dichos órganos administrativos, organismos y entidades una certificación del contenido de las condiciones específicas aplicables a un tipo de información pública en un momento determinado. Esta certificación será expedida preferentemente mediante medios electrónicos y, en todo caso, en un plazo máximo de 15 días.

4. La modalidad de puesta a disposición previa solicitud conforme al párrafo c) del apartado 2 del artículo 4 de la Ley 37/2007, de 16 de noviembre, se empleará, con carácter general, cuando la naturaleza de los documentos reutilizables exija la tramitación de un procedimiento previa solicitud conforme al artículo 10 de la Ley 37/2007, de 16 de noviembre, por ejemplo, cuando no preexistan en formato electrónico, y en otros casos excepcionales que sean definidos de manera motivada en la correspondiente orden ministerial o resolución del presidente del organismo o entidad correspondiente. Este procedimiento será tramitado preferentemente por medios electrónicos en los términos establecidos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y su normativa de desarrollo, figurando el acceso al mismo entre la información sobre la documentación susceptible de ser reutilizada descrita en el artículo 4.

## CAPÍTULO IV

## Régimen aplicable a documentos reutilizables sujetos a derechos de propiedad intelectual o que contengan datos personales

**Artículo 9.** *Documentos e información objeto de derechos de propiedad intelectual o industrial de terceros.*

La reutilización de los documentos que custodian los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 sobre los que existan derechos de propiedad intelectual o industrial de terceros sólo podrá ser autorizada si tales órganos, organismos y entidades disponen u obtienen, cuando la reutilización concreta que se vaya a hacer lo exija y en los términos en que sea necesaria, la preceptiva y suficiente cesión de los derechos de explotación por parte de sus titulares.

**Artículo 10.** *Ejercicio de los derechos de propiedad intelectual de titularidad de los órganos administrativos, organismos o entidades del sector público estatal.*

1. De acuerdo con lo establecido en el artículo 3.3.e) de la Ley 37/2007, de 16 de noviembre, los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 deben ejercer sus derechos de propiedad intelectual sobre sus documentos de forma que se facilite su reutilización.

2. A tal efecto, la puesta a disposición de dichos documentos para su reutilización realizada conforme a lo dispuesto en el artículo 8.1 conllevará la cesión gratuita y no exclusiva de los derechos de propiedad intelectual correspondientes necesarios para

desarrollar la actividad de reutilización autorizada, en cualquier modalidad y bajo cualquier formato, para todo el mundo y por el plazo máximo permitido por la Ley.

No obstante, lo dispuesto en el párrafo anterior podrá ser excepcionado, en todo lo no referente a la no exclusividad de la cesión, mediante el establecimiento de condiciones específicas de acuerdo con lo dispuesto en los apartados 2 a 4 del artículo 8 cuando se empleen las modalidades de puesta a disposición previstas en los mismos, siempre dentro de los límites establecidos en la Ley 37/2007, de 16 de noviembre, y, en particular, en su artículo 4.3 y en su artículo 6.

**Artículo 11.** *Reutilización de los documentos que contengan datos de carácter personal.*

1. El acceso a documentos que contengan datos de carácter personal o referentes a la intimidad de las personas estará reservado a éstas, que podrán además ejercer sus derechos de rectificación, cancelación y oposición de acuerdo con lo previsto en la legislación de protección de datos personales y el artículo 37.2 de la Ley 30/1992, de 26 de noviembre.

2. No obstante, siempre y cuando los medios técnicos y económicos lo permitan, deberá procederse a la disociación de los datos personales, en los términos que se derivan de lo establecido en el artículo 3.f) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en el artículo 5.1.e) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba su Reglamento de Desarrollo, a fin de permitir su reutilización por otras personas.

**Disposición adicional primera.** *Ausencia de impacto presupuestario.*

La aplicación de las previsiones contenidas en este real decreto no supondrá incremento del gasto público ni disminución de los ingresos públicos. Por tanto, los departamentos ministeriales, organismos y entidades afectados deben desarrollar las medidas derivadas de su cumplimiento ateniéndose a sus disponibilidades presupuestarias ordinarias, no dando lugar, en ningún caso, a planteamientos de necesidades adicionales de financiación.

**Disposición adicional segunda.** *Adaptación del sector público estatal a las disposiciones de este real decreto.*

Los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal a que se hace referencia en el artículo 1.2 deberán adaptarse a las disposiciones de este real decreto en el plazo de un año desde su entrada en vigor.

En el citado plazo de un año, aprobarán un plan propio de medidas de impulso de la reutilización de la información del sector público por medios electrónicos, dentro de su ámbito de competencias, que incluirá el compromiso por parte de los departamentos ministeriales de publicar a través de tales medios, de una manera estructurada y usable para los interesados e interesadas y en bruto, en formatos procesables y accesibles de modo automatizado correspondientes a estándares abiertos, al menos cuatro conjuntos de documentos de alto impacto y valor en un plazo máximo de seis meses desde la finalización del plazo de adaptación previsto en el párrafo anterior.

**Disposición final primera.** *Modificación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.*

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, se modifica como sigue:

Uno. Se añade un nuevo párrafo l) al apartado 1 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, que tendrá la siguiente redacción:

> «l) Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de

información puestos a disposición del público por medios electrónicos para su reutilización.»

Dos. Se añade una nueva disposición adicional con la siguiente redacción:

**«Disposición adicional quinta.** *Normativa técnica relativa a la reutilización de recursos de información.*

La normativa relativa a la reutilización de recursos de información deberá estar aprobada a más tardar el 1 de junio de 2012.»

**Disposición final segunda.** *Habilitación para el desarrollo normativo.*

Por los Ministros de Industria, Turismo y Comercio y de Política Territorial y Administración Pública, se dictarán conjunta o separadamente, según las materias de que se trate, y en el ámbito de sus respectivas competencias, las disposiciones que exijan el desarrollo y aplicación de este real decreto.

**Disposición final tercera.** *Autorización para la modificación del anexo.*

Se autoriza a que mediante orden del Ministro de la Presidencia, a propuesta conjunta de los Ministros de Industria, Turismo y Comercio, y de Política Territorial y Administración Pública pueda modificarse el contenido del anexo de este real decreto, a fin de mantenerlo actualizado.

**Disposición final cuarta.** *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## ANEXO

### Aviso legal para la modalidad general de puesta a disposición de los documentos reutilizables regulada en el apartado 1 del artículo 8

1. Conforme a lo dispuesto en el artículo 7 del presente real decreto se incluirá el siguiente texto en el aviso legal disponible por medios electrónicos, preferentemente en la ubicación «sede.gob.es/datosabiertos» de la sede electrónica del órgano administrativo, organismo o entidad correspondiente.

«Obligatoriedad de las condiciones generales.

Las presentes condiciones generales, disponibles con carácter permanente bajo “www.datos.gob.es/avisolegal”, vincularán a cualquier agente reutilizador por el mero hecho de hacer uso de los documentos sometidos a ellas.

Autorización de reutilización y cesión no exclusiva de derechos de propiedad intelectual.

Las presentes condiciones generales permiten la reutilización de los documentos sometidos a ellas para fines comerciales y no comerciales. Se entiende por reutilización el uso de documentos que obran en poder de los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 del Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público estatal, por personas físicas o jurídicas, con fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública. La reutilización autorizada incluye, a modo ilustrativo, actividades como la copia, difusión, modificación, adaptación, extracción, reordenación y combinación de la información.

El concepto de documento es el establecido en el apartado 2 del artículo 3 de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, por lo que comprende toda información cualquiera que sea su soporte material o electrónico así como su forma de expresión gráfica, sonora o en imagen utilizada, incluyendo, en consecuencia, también los datos en sus niveles más desagregados o “en bruto”.

Esta autorización conlleva, asimismo, la cesión gratuita y no exclusiva de los derechos de propiedad intelectual, en su caso, correspondientes a tales documentos, autorizándose la realización de actividades de reproducción, distribución, comunicación pública o transformación, necesarias para desarrollar la actividad de reutilización autorizada, en cualquier modalidad y bajo cualquier formato, para todo el mundo y por el plazo máximo permitido por la Ley.

Condiciones generales para la reutilización.

Son de aplicación las siguientes condiciones generales para la reutilización de los documentos sometidos a ellas:

1. Está prohibido desnaturalizar el sentido de la información.
2. Debe citarse la fuente de los documentos objeto de la reutilización. Esta cita podrá realizarse de la siguiente manera: "Origen de los datos: [*órgano administrativo, organismo o entidad del sector público estatal de que se trate*]".
3. Debe mencionarse la fecha de la última actualización de los documentos objeto de la reutilización, siempre cuando estuviera incluida en el documento original.
4. No se podrá indicar, insinuar o sugerir que la [*órgano administrativo, organismo o entidad del sector público estatal de que se trate*] titular de la información reutilizada participa, patrocina o apoya la reutilización que se lleve a cabo con ella.
5. Deben conservarse, no alterarse ni suprimirse los metadatos sobre la fecha de actualización y las condiciones de reutilización aplicables incluidos, en su caso, en el documento puesto a disposición para su reutilización.

Exclusión de responsabilidad.

La utilización de los conjuntos de datos se realizará por parte de los usuarios o agentes de la reutilización bajo su propia cuenta y riesgo, correspondiéndoles en exclusiva a ellos responder frente a terceros por daños que pudieran derivarse de ella.

[El *órgano administrativo, organismo o entidad del sector público estatal de que se trate*] no será responsable del uso que de su información hagan los agentes reutilizadores ni tampoco de los daños sufridos o pérdidas económicas que, de forma directa o indirecta, produzcan o puedan producir perjuicios económicos, materiales o sobre datos, provocados por el uso de la información reutilizada.

[El *órgano administrativo, organismo o entidad del sector público estatal de que se trate*] no garantiza la continuidad en la puesta a disposición de los documentos reutilizables, ni en contenido ni en forma, ni asume responsabilidades por cualquier error u omisión contenido en ellos.

Responsabilidad del agente reutilizador

El agente reutilizador se halla sometido a la normativa aplicable en materia de reutilización de la información del sector público, incluyendo el régimen sancionador previsto en el artículo 11 de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.»

2. Con el objetivo de informar a los motores y sistemas automatizados de búsqueda en Internet, se incorporarán además en la codificación de la citada ubicación los mecanismos de localización de información pública reutilizable que se estimen oportunos. Para ello, si bien se podrán utilizar otras modalidades técnicas, se propone el siguiente comando básico, que enlaza con las condiciones generales de reutilización:

<a href="http://www.datos.gob.es/avisolegal" rel="license">Aviso legal</a>

o bien el comando

<a href="http://www.datos.gob.es/avisolegal">Aviso legal</a>.

# § 6

## Orden EHA/1049/2008, de 10 de abril, de declaración de bienes y servicios de contratación centralizada

Ministerio de Economía y Hacienda
«BOE» núm. 93, de 17 de abril de 2008
Última modificación: 6 de agosto de 2022
Referencia: BOE-A-2008-6804

Téngase en cuenta que las referencias efectuadas en esta Orden a la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, se entenderán referidas a los correspondientes artículos del texto refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre, según establece la disposición adicional única de la Orden HAP/19/2014, de 13 de enero. Ref. BOE-A-2014-439.
El Real Decreto Legislativo 3/2011 citado ha sido derogado, con efectos de 9 de marzo de 2018, por la disposición derogatoria de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público. Ref. BOE-A-2017-12902

La Ley 42/2006, de 28 de diciembre, de Presupuestos Generales del Estado para el año 2007, modificó el artículo 182 g) del Texto Refundido de la Ley de Contratos de las Administraciones Públicas, aprobado por Real Decreto Legislativo 2/2000, de 16 de junio, en el sentido de limitar el recurso al procedimiento negociado sin publicidad para la adjudicación de los contratos que se refieran a bienes cuya uniformidad haya sido declarada necesaria para su utilización común por la Administración.

Como consecuencia de esta modificación se dictó la Orden Ministerial EHA/2/2007, de 9 de enero, de declaración de bienes y servicios de contratación centralizada, con objeto de regular el procedimiento de contratación centralizada de forma transitoria hasta la entrada en vigor de la Ley de Contratos del Sector Público, avanzando ya dicho texto la necesidad de proceder a la redacción de una nueva Orden de centralización reguladora de dicho procedimiento y acorde con los cambios establecidos en la nueva legislación.

La Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, que transpone la Directiva 2004/18/CE, del Parlamento Europeo y del Consejo, de 31 de marzo de 2004, sobre coordinación de los procedimientos de adjudicación de los contratos públicos de obras, de suministro y de servicios, incorpora entre otros elementos una nueva regulación de la contratación centralizada dando cabida no sólo a los hasta ahora contemplados contratos de suministro y de servicios sino también a la posible centralización de los contratos de obras. Por otra parte la nueva ley modifica la tipología de los contratos, eliminando la diferenciación existente en la normativa anterior entre los contratos de servicios y los de asistencia técnica y consultoría, encontrándose a partir de ahora unos y otros englobados en la categoría única de contratos de servicios.

Esta Ley también establece de manera específica la competencia de la Dirección General del Patrimonio del Estado para operar como central de contratación única en el ámbito de la Administración General del Estado, sus Organismos autónomos, Entidades gestoras y Servicios comunes de la Seguridad Social y demás Entidades públicas estatales. Para llevar a cabo esta función introduce sistemas para la racionalización técnica de la contratación aplicables en concreto a la contratación centralizada, tales como el acuerdo marco y el sistema dinámico de contratación.

Asimismo, y con motivo de la entrada en vigor de la Ley de Contratos del Sector Público, es necesario concretar el régimen transitorio de los concursos de adopción de tipo adjudicados al amparo del antiguo texto legal.

Estas circunstancias hacen necesaria la redefinición del ámbito al que se extiende la contratación centralizada. En consecuencia, y haciendo uso de la competencia atribuida por el artículo 190.1 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, previo informe de la Comisión Permanente de la Junta Consultiva de Contratación Administrativa, dispongo:

**Artículo 1.** *Declaración de suministros de contratación centralizada.*

En el ámbito establecido en el artículo 206.1 del texto refundido de la Ley de Contratos del Sector Público aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, se declaran de contratación centralizada los contratos de suministros que a continuación se relacionan:

a) Mobiliario de despacho y complementario, de archivo, de bibliotecas, mamparas, clínico, de laboratorio y otros de uso común de la Administración.

b) Ordenadores personales, servidores y sistemas de almacenamiento y elementos complementarios.

c) Software de sistema, de desarrollo y de aplicación.

d) Equipos de impresión, sus elementos complementarios así como el material fungible que se contrate asociado directamente con dichos equipos.

e) Fotocopiadoras, copiadoras, multicopiadoras, sus elementos complementarios y el material fungible.

f) Equipos de destrucción de documentos.

g) Papel de equipos de impresión, fotocopiadoras, copiadoras y multicopiadoras.

h) Equipos audiovisuales.

i) Equipos y programas de telecomunicación para la transmisión de voz y datos.

j) Equipos de control de acceso de personas y paquetería.

k) Sistemas contra intrusión, antirrobo y contra incendios.

l) Equipos de seguridad electrónica y física.

m) Vehículos a motor para transporte de personas y mercancías, tales como motocicletas, automóviles de turismo, todo terreno, vehículos industriales y autobuses con cualquier clase de equipamiento específico.

n) Combustibles en estaciones de servicio.

o) Energía eléctrica, con exclusión de aquellos suministros que puedan tramitarse mediante contrato menor.

p) Material de oficina no inventariable.

**Artículo 2.** *Declaración de servicios de contratación centralizada.*

En el ámbito establecido en el artículo 206.1 del texto refundido de la Ley de Contratos del Sector Público aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, se declaran de contratación centralizada los contratos de servicios que a continuación se relacionan:

a) Los servicios dirigidos al desarrollo de la Administración Electrónica cuyo presupuesto de licitación no supere 862.000 euros, I.V.A. excluido, cuyo objeto consista en:

1. Trabajos de consultoría, planificación, estudio de viabilidad, análisis, diseño, construcción e implantación de sistemas de información, y los mantenimientos de las aplicaciones desarrolladas bajo esta modalidad.

2. Servicios de alojamiento en sus distintas modalidades, y los servicios remotos de explotación y control de sistemas de información que den soporte a servicios públicos de administración electrónica.

b) Los servicios de telecomunicaciones.

c) Los servicios dirigidos a la compra de espacios en medios de comunicación y demás soportes publicitarios relativos a campañas de publicidad institucional, con exclusión de aquellos cuyas características puedan tener la consideración de contrato menor.

d) Los servicios de seguridad privada y de servicios de auxiliares de control, con exclusión de aquellos cuyas características puedan tener la consideración de contrato menor.

e) Los servicios de limpieza integral de edificios.

f) Los servicios postales, con exclusión de aquellos cuyas características puedan tener la consideración de contrato menor.

g) Los servicios de agencias de viajes.

h) Los servicios de evaluación ex post de la eficacia de las campañas de publicidad institucional de la Administración General del Estado y demás entidades del sector público estatal incluidas en el ámbito de la Ley 29/2005, de 29 de diciembre, de Publicidad y Comunicación Institucional cuya difusión se desarrolle dentro del territorio nacional, con exclusión de las campañas incluidas en el correspondiente Plan Anual de Publicidad Institucional que no tengan coste, las campañas incluidas en los supuestos previstos en el artículo cincuenta de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General y las campañas institucionales cuya evaluación sea preceptiva y deba adecuarse a condiciones específicas de conformidad con la normativa de la Unión Europea.

Asimismo, se excluye de la presente centralización la evaluación ex post de aquellas campañas cuya contratación de compra de espacios en medios de comunicación y demás soportes publicitarios hubieran tenido la consideración de contrato menor.

i) Los servicios de ciberseguridad.

j) Los servicios de actualización y de soporte del software mencionado en la letra c) del artículo anterior.

**Artículo 3.** *Procedimiento de contratación.*

La contratación de los bienes y servicios declarados de contratación centralizada será efectuada por la Dirección General de Racionalización y Centralización de la Contratación mediante la celebración de acuerdos marco, la articulación de sistemas dinámicos de adquisición o la conclusión de contratos que se adjudicarán con arreglo a las normas procedimentales contenidas en el texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre.

La concreción de la técnica o técnicas de centralización de la contratación aplicable a cada servicio o suministro, será determinado mediante resolución del titular de la Dirección General de Racionalización y Centralización de la Contratación.

Con relación a los contratos basados, la propuesta de adjudicación, independientemente de si requieren o no de una nueva licitación, se realizará por medios telemáticos a través de la aplicación CONECTA CENTRALIZACIÓN junto con la documentación requerida en cada caso. Con carácter preceptivo deberá adjuntarse la propuesta de adjudicación firmada por el organismo interesado u órgano gestor competente y diligenciado, en su caso, por el Interventor delegado en relación con la fiscalización del expediente.

**Artículo 4.** *Autorizaciones de contratación al margen de los acuerdos marcos o sistemas dinámicos de contratación de la Central de Contratación del Estado.*

Con carácter previo a la entrada en vigor del acuerdo marco o del sistema dinámico de contratación, la contratación de los servicios, suministros u obras declarados centralizados al margen de la Central de Contratación del Estado será realizada por el órgano competente conforme a las normas generales de competencia y procedimiento siempre que esos contratos no tengan una duración superior a un año, prorrogable por, como máximo, otro año. En todo caso, para poder acordar la prórroga será necesario el informe favorable de la Dirección General de Racionalización y Centralización de la Contratación.

Atendiendo a razones de eficiencia en la gestión y a solicitud del órgano de contratación afectado, la Dirección General de Racionalización y Centralización de la Contratación podrá autorizar la excepción a esta limitación temporal.

En los acuerdos marco o sistemas dinámicos de contratación vigentes, la contratación de los servicios o suministros incluidos en el ámbito objetivo del mismo al margen de la Central de Contratación del Estado sólo podrá ser realizada por el órgano competente conforme a las normas generales de competencia y procedimiento, previo informe favorable de la Dirección General de Racionalización y Centralización de la Contratación. Este informe favorable se emitirá cuando se acredite que los bienes adjudicados o el régimen de prestación de los servicios establecido no reúnen las características indispensables para satisfacer las concretas necesidades del organismo peticionario.

**Artículo 5.** *Autorizaciones de contratación al margen de los contratos centralizados de la Central de Contratación del Estado.*

Cuando la técnica de articulación de la centralización de la contratación de un servicio, suministro u obra sea mediante la conclusión de un contrato, la contratación de estos servicios, suministros u obras al margen de la Central de Contratación del Estado, o la prórroga de contratos vigentes desde la entrada en vigor de la resolución que declare la centralización de la contratación de los servicios, suministros u obras correspondientes por el titular del Ministerio de Hacienda y Administraciones Públicas, sólo podrá ser realizada cuando se justifique por las características del servicio, del suministro o de la obra, del organismo peticionario o por razones de planificación de la propia centralización de la contratación, por el órgano competente conforme a las normas generales de competencia y procedimiento y, en todo caso, previo informe favorable de la Dirección General de Racionalización y Centralización de la Contratación.

**Artículo 6.** *Concepto de organismo interesado.*

El artículo 206.3 del texto refundido de la Ley de Contratos del Sector Público establece que cuando la contratación de los suministros, servicios u obras deba efectuarse convocando a las partes en un acuerdo marco a una nueva licitación conforme a lo previsto en las letras a) a d) del apartado 4 del artículo 198, la consulta por escrito a los empresarios capaces de realizar la prestación, así como la recepción y examen de las proposiciones serán responsabilidad del organismo interesado en la adjudicación del contrato, que elevará la correspondiente propuesta a la Dirección General del Racionalización y Centralización de la Contratación.

Teniendo en cuenta las diversas posibilidades de configuración de los contratos basados, el concepto de organismo interesado en la adjudicación puede referirse en cada caso a distintos organismos. A estos efectos, se distinguen los siguientes supuestos cuando el órgano de contratación sea la Dirección General de Racionalización y Centralización de la Contratación:

a) En la adjudicación de los contratos basados en acuerdos marco en los que sólo exista un destinatario de los servicios, suministros u obras, será este destinatario el que tenga la consideración de organismo interesado.

b) En la adjudicación de los contratos basados en acuerdos marco en los que se tenga por destinatarios de los servicios, suministros u obras a varios departamentos u organismos:

b.1) La Dirección General de Racionalización y Centralización de la Contratación podrá adoptar la decisión de iniciar un procedimiento para la adjudicación de un contrato basado que tenga por destinatarios varios departamentos u organismos si se considera conveniente por razones de eficacia en el cumplimiento de los objetivos o de eficiencia en la gestión y utilización de los recursos públicos. En estos casos, tendrá la consideración de organismo interesado la Dirección General de Racionalización y Centralización de la Contratación, salvo que los destinatarios sean un departamento ministerial y organismos vinculados o dependientes de éste, en cuyo caso, la consideración de organismo interesado la tendrá el departamento ministerial.

b.2) Por las mismas razones de eficacia y eficiencia, la Dirección General de Racionalización y Centralización de la Contratación podrá adoptar la decisión de solicitar

oferta que se aplicará a los contratos basados que correspondan a cada uno de los departamentos u organismos destinatarios de los bienes o servicios incluidos en dicha solicitud de oferta. En estos casos, la Dirección General de Racionalización y Centralización de la Contratación actuará como organismo interesado.

Por su parte, cada uno de los departamentos u organismos destinatarios tramitará el correspondiente expediente financiero de gasto para atender sus necesidades de acuerdo a lo indicado en la oferta.

**Artículo 7.** *Objeto de los acuerdos de adhesión.*

Las Comunidades Autónomas, las Entidades Locales, los organismos autónomos y entes públicos dependientes de ellas y el resto de entidades del sector público estatal no incluidos en el artículo 206.1 del texto refundido de la Ley de Contratos del Sector Público, aprobado mediante Real Decreto Legislativo 3/2011, de 14 de noviembre, podrán adherirse voluntariamente a la Central de Contratación del Estado para la totalidad de los servicios, suministros y obras declarados centralizados o sólo para determinadas categorías de ellos, articulándose a través de acuerdos de adhesión.

**Artículo 8.** *Procedimiento de adhesión.*

El procedimiento de adhesión se realizará en dos fases.

En una primera fase, la Comunidad Autónoma, Entidad Local, organismo autónomo o ente público dependiente de ella o, en su caso, el resto de entidades del sector público estatal no incluidas en el ámbito obligatorio de aplicación, de acuerdo con el artículo 229.2 de la Ley 9/2017, de 8 de noviembre, suscribirán con la Dirección General de Racionalización y Centralización de la Contratación un acuerdo de adhesión genérico a la Central de Contratación del Estado.

La celebración de este acuerdo de adhesión genérico implicará la manifestación formal de su voluntad de integrarse en el régimen general de funcionamiento de la Central de Contratación del Estado y el derecho de adherirse a los distintos acuerdos marco o sistemas dinámicos de adquisición de la Central de Contratación del Estado.

En una segunda fase, la entidad formalizará la adhesión voluntaria a un acuerdo marco o un sistema dinámico de adquisición específico, lo que implicará la obligación del ente o entidad adherida de realizar todas las contrataciones a través del mismo salvo cuando los bienes adjudicados o el régimen de prestación de los servicios no reúna las características indispensables para satisfacer las concretas necesidades del ente o entidad individualmente adherido. Esta circunstancia requerirá información trimestral a la Dirección General de Racionalización y Centralización de la Contratación.

La Dirección General de Racionalización y Centralización de la Contratación está obligada a facilitar el acceso a la aplicación informática CONECTA-CENTRALIZACIÓN a los entes y entidades que se adhieran voluntariamente a un acuerdo marco o a un sistema dinámico de adquisición específico.

Es obligación de los entes adheridos diligenciar la propuesta de adjudicación por el órgano de control interno de la gestión económica-financiera de las entidades sujetas a función interventora. Por otro lado, tienen derecho a recibir información individualizada de los acuerdos marcos y sistema dinámico de adquisición a celebrar a fin de solicitar su adhesión específica a los mismos.

El período de vigencia del acuerdo específico de adhesión será equivalente al del acuerdo marco o sistema dinámico de adquisición de referencia.

La Dirección General de Racionalización y Centralización de la Contratación publicará a través del portal contratación centralizada los modelos de acuerdo de adhesión genéricos y específicos.

**Artículo 9.** *Junta de Contratación Centralizada.*

La Junta de Contratación Centralizada es el órgano de contratación del sistema estatal de contratación centralizada de conformidad con el artículo 316.3 del texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, sin perjuicio de la desconcentración de competencias prevista en la disposición

adicional quinta del Real Decreto 696/2013, de 20 de septiembre, por el que se modifica el Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas.

Se encuentra adscrita a la Dirección General de Racionalización y Centralización de la Contratación.

**Artículo 10.** *Composición y funcionamiento de la Junta de Contratación Centralizada.*

La Junta de Contratación Centralizada actuará en Pleno o en Comisión Permanente, como órgano de contratación colegiado en el ámbito de las competencias atribuidas por el ordenamiento jurídico. El Pleno ejercerá las funciones que le atribuye el ordenamiento jurídico, salvo las asignadas a la Comisión Permanente en el artículo 12 de esta Orden.

La Junta de Contratación Centralizada contará, para el ejercicio de sus funciones, con una Secretaría que le prestará apoyo administrativo cuando actúe en Pleno y en Comisión Permanente.

**Artículo 11.** *Composición y funcionamiento del Pleno de la Junta de Contratación Centralizada.*

1. El Pleno de la Junta de Contratación Centralizada estará compuesto por los siguientes miembros:

a) Presidente: el titular de la Dirección General de Racionalización y Centralización de la Contratación.

b) Vocales:

1. Dos vocales pertenecientes a la Dirección General de Racionalización y Centralización de la Contratación, con rango de Subdirector General, nombrados por el titular de la Subsecretaría de Hacienda y Administraciones Publicas a propuesta del titular de la Dirección General de Racionalización y Centralización de la Contratación.

2. Dos vocales designados por el titular de la Subsecretaría de Hacienda y Administraciones Públicas, uno a propuesta del titular de la Subsecretaría del Ministerio de Presidencia en representación de este Ministerio y otro a su propia iniciativa en representación del Ministerio de Hacienda y Administraciones Públicas.

3. Tres vocales en representación del resto de los departamentos ministeriales. La asistencia de los representantes designados por cada departamento, por el mismo procedimiento del apartado anterior, tendrá carácter rotatorio trimestral. El orden de asistencia entre los Departamentos será el previsto en el Real Decreto 1823/2011, de 21 de diciembre, por el que se reestructuran los departamentos ministeriales.

Así mismo, podrán ser convocados al Pleno de la Junta de Contratación Centralizada, representantes de otros departamentos ministeriales, a los que no les corresponda su asistencia conforme al párrafo anterior, cuando éste haya de tratar aspectos relacionados con contratos que tengan una singular incidencia en dichos ministerios. Estos representantes serán los nombrados para la asistencia a la Junta de Contratación Centralizada y actuarán con voz pero sin voto.

4. Un Abogado del Estado de la Abogacía del Estado en el Ministerio de Hacienda y Administraciones Públicas.

5. Un Interventor de la Intervención Delegada en el Ministerio de Hacienda y Administraciones Públicas.

c) Secretario: el Subdirector General que tenga atribuidas dichas funciones, que actuará como vocal, con voz y voto.

2. El régimen de sustituciones en caso de vacancia, ausencia o enfermedad y, en general, cuando concurra una causa justificada, será el siguiente:

a) El Presidente será sustituido por el vocal que se determine en cada momento mediante resolución del titular de la Dirección General de Racionalización y Centralización de la Contratación. En su defecto, por el orden establecido en el nombramiento como vocales efectuado por el titular de la Subsecretaría de Hacienda y Administraciones Publicas

a propuesta del titular de la Dirección General de Racionalización y Centralización de la Contratación.

b) Los vocales pertenecientes a la Dirección General de Racionalización y Centralización de la Contratación y los vocales representantes de los distintos departamentos ministeriales serán sustituidos por sus suplentes, que serán nombrados por el mismo procedimiento.

c) El Secretario será sustituido por el funcionario de la Dirección General que nombre el titular de la Dirección General de Racionalización y Centralización de la Contratación.

3. A las reuniones podrán asistir los funcionarios o asesores especializados que resulten necesarios para el análisis de los expedientes de contratación, según la naturaleza de los asuntos a tratar, los cuales actuarán con voz pero sin voto.

4. El funcionamiento del Pleno se ajustará a la normativa contractual vigente para los órganos de contratación y, con carácter supletorio, a las normas de los órganos colegiados que se establecen en el capítulo II del título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

5. Si en relación con actos dictados por el Pleno de la Junta de Contratación Centralizada o por la Comisión Permanente se interpusiese una cuestión de nulidad de las previstas en el artículo 37 del texto refundido de la Ley de Contratos del Sector Público o un recurso especial en materia de contratación de los previstos en el artículo 40 de dicho texto refundido, el Presidente del Pleno emitirá cuantos informes sean exigidos por el ordenamiento jurídico. En caso de vacante, ausencia o enfermedad y, en general, cuando concurra alguna causa justificada, será el Secretario quien emita los citados informes.

**Artículo 12.** *Comisión Permanente de la Junta de Contratación Centralizada.*

1. La Comisión Permanente estará compuesta por los siguientes miembros:

a) Presidente: El titular de la Dirección General de Racionalización y Centralización de la Contratación.

b) Vocales:

1. Dos vocales pertenecientes a la Dirección General de Racionalización y Centralización de la Contratación, con rango de Subdirector General, nombrados por el titular de la Subsecretaría de Hacienda y Administraciones Públicas a propuesta del titular de la Dirección General de Racionalización y Centralización de la Contratación.

Así mismo, podrán ser convocados a la Comisión Permanente de la Junta de Contratación Centralizada, como vocales con voz pero sin voto, representantes de los Departamentos Ministeriales cuando ésta haya de tratar aspectos relacionados con contratos que tengan una singular incidencia en dichos ministerios. Estos representantes serán los nombrados para la asistencia al Pleno de la Junta de Contratación Centralizada.

2. Un Abogado del Estado de la Abogacía del Estado en el Ministerio de Hacienda y Administraciones Públicas.

3. Un Interventor de la Intervención Delegada en el Ministerio de Hacienda y Administraciones Públicas.

c) Secretario: El Secretario del pleno con voz pero sin voto

2. El régimen de sustituciones en caso de vacancia, ausencia o enfermedad y, en general, cuando concurra una causa justificada, será el siguiente:

a) El Presidente será sustituido por el vocal que se determine en cada momento mediante resolución del titular de la Dirección General de Racionalización y Centralización de la Contratación. En su defecto, por el orden establecido en el nombramiento como vocales efectuado por el titular de la Subsecretaría de Hacienda y Administraciones Publicas a propuesta del titular de la Dirección General de Racionalización y Centralización de la Contratación.

b) Los vocales pertenecientes a la Dirección General de Racionalización y Centralización de la Contratación serán sustituidos por sus suplentes, que serán nombrados por el mismo procedimiento.

c) El Secretario será sustituido por el funcionario de la Dirección General que designe el titular de la Dirección General de Racionalización y Centralización de la Contratación.

3. Las funciones atribuidas a la Comisión Permanente son las previstas para las mesas de contratación en el artículo 22 del Real Decreto 817/2009, de 8 de mayo, por el que se desarrolla parcialmente la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público y en otras disposiciones normativas. Asimismo, la Comisión Permanente podrá ejercer, previa delegación, las funciones atribuidas al Pleno de la Junta de Contratación Centralizada.

Adicionalmente, en aquellos expedientes de adquisición centralizada de equipos y sistemas para el tratamiento de la información en los que el titular de la Dirección General de Racionalización y Centralización de la Contratación actúe como órgano de contratación, la Comisión Permanente ejercerá las funciones de mesa de contratación, cuando sea preceptiva su participación o potestativamente así se determine.

4. A las reuniones podrán incorporarse los funcionarios o asesores especializados que resulten necesarios para el análisis y valoración de las ofertas, según la naturaleza de los asuntos a tratar, los cuales actuarán con voz pero sin voto.

5. El funcionamiento de la Comisión Permanente se ajustará a la normativa contractual vigente para las mesas de contratación y órganos de contratación, según proceda en cada caso, y con carácter supletorio, a las normas de los órganos colegiados que se establecen en el capítulo II del título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

6. La Comisión Permanente podrá constituir los grupos de trabajo que considere oportunos para la preparación de los documentos que deban ser estudiados y aprobados por ella. En todo caso, el resultado de estas actuaciones deberá ser ratificado por la Comisión Permanente.

**Artículo 13.** *La Secretaría de la Junta de Contratación Centralizada.*

1. La Secretaría de la Junta de Contratación Centralizada prestará el apoyo administrativo necesario para el adecuado desarrollo de las funciones asignadas a la Junta de Contratación Centralizada, ya actúe en Pleno o en Comisión Permanente.

2. Las funciones de la Secretaría son las siguientes, además de las previstas en el artículo 25 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común:

a) Remitir la información y documentación así como realizar las peticiones que sean necesarias respecto a los procedimientos tramitados por el Tribunal Administrativo Central de Recursos Contractuales.

b) Remitir la información que se requiera respecto a los expedientes tramitados por la Junta de Contratación Centralizada al Registro de Contratos del Sector Público así como la documentación que proceda respecto a dichos expedientes al Tribunal de Cuentas.

c) Gestionar el perfil del contratante de la Plataforma de Contratación del Sector Público.

d) Dar cumplimiento mediante los requerimientos de documentación o comunicaciones que procedan a los acuerdos del Pleno y/o de la Comisión Permanente de la Junta de Contratación Centralizada.

e) En general, todas aquellas otras funciones que contribuyan a la consecución de los fines y objetivos de los órganos colegiados en materia de contratación.

**Disposición adicional primera.** *Tramitación de solicitudes a través de Conecta Centralización.*

En el ámbito del sector público estatal, las solicitudes de contratos basados en el acuerdo marco o de adjudicaciones de contratos realizados en el marco del sistema dinámico de contratación se tramitarán, a través de la aplicación informática CONECTA CENTRALIZACIÓN.

A partir del 1 de junio de 2016 esta obligación se extenderá a los entes que no forman parte del sector público estatal.

**Disposición adicional segunda.** *Coordinación de la vigencia de determinados contratos.*

La Administración General del Estado y demás entidades comprendidas en el ámbito subjetivo obligatorio de la Central de Contratación del Estado deberán recabar el informe favorable de la Dirección General de Racionalización y Centralización de la Contratación para tramitar contratos cuya duración sea superior a un año, prorrogable por un año adicional, cuando su objeto consista en aquellos suministros, obras y servicios que, por Resolución de la citada Dirección General, se identifiquen como susceptibles de ser próximamente declarados de contratación centralizada por el Ministro de Hacienda y Función Pública, de conformidad con lo dispuesto en el artículo 229.1 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

**Disposición transitoria primera.** *Régimen aplicable a los contratos derivados de concursos de adopción de tipo.*

Los contratos derivados de los concursos de adopción de tipo vigentes a la entrada en vigor de la Ley de Contratos del Sector Público se adjudicarán por el procedimiento previsto para la adjudicación de contratos basados en un acuerdo marco en el artículo 182.4 de la Ley de Contratos del Sector Público. A tal efecto se entenderá por términos del acuerdo marco los establecidos en las respectivas adjudicaciones de los concursos de adopción de tipo.

**Disposición transitoria segunda.** *Régimen transitorio de los contratos relativos a seguridad privada y auxiliares de control.*

En tanto la Dirección General de Racionalización y Centralización de la Contratación no lo determine, la centralización de los contratos de seguridad y auxiliares de control afectará únicamente a los servicios que se presten en bienes inmuebles situados en el municipio de Madrid ocupados principalmente por unidades administrativas. No obstante, en estos contratos, a propuesta de los Ministerios u organismos afectados, podrán incluirse inmuebles de distinto ámbito territorial o uso cuando su gestión esté atribuida a dichas unidades y la contratación conjunta resulte más eficiente.

Por tanto, durante este periodo transitorio, la contratación al margen del sistema estatal de contratación centralizada de los servicios de seguridad que se vayan a prestar en distinto ámbito geográfico y uso al referido en el párrafo anterior no requerirá el informe favorable al que se refiere el artículo quinto.

**Disposición transitoria tercera.** *Régimen transitorio de los contratos relativos a la limpieza integral de edificios.*

En tanto la Dirección General de Racionalización y Centralización de la Contratación no lo determine, la centralización de los contratos de limpieza integral de edificios afectará únicamente a los servicios que se presten en bienes inmuebles situados en el territorio de la Comunidad de Madrid cuyo uso principal sea administrativo, judicial o laboratorio.

Por tanto, no se aplicará hasta ese momento el régimen previsto en el artículo 5 cuando la prestación del servicio se desarrolle en bienes inmuebles situados fuera del ámbito territorial indicado, o cuando el uso exclusivo de los citados bienes sea museos, teatros, auditorios, cines, bibliotecas, centros deportivos, centros hospitalarios, residencias, fincas rústicas, instalaciones militares y de transporte, centros penitenciarios, comisarías o sean bienes integrantes del Patrimonio Nacional, de acuerdo con la Ley 23/1982, de 16 de junio, reguladora del Patrimonio Nacional.

En caso de uso mixto, si los inmuebles se encuentran dentro del ámbito territorial indicado, será necesario el informe favorable de la Dirección General de Racionalización y Centralización de la Contratación, con carácter previo al inicio del expediente de contratación.

**Disposición derogatoria única.** *Régimen de derogaciones.*

A la entrada en vigor de la presente Orden quedará derogada la Orden EHA/2/2007, de 9 de enero, de declaración de bienes y servicios de contratación centralizada.

**Disposición final única.** *Entrada en vigor.*

Esta Orden entrará en vigor el día 2 de mayo de 2008.

# § 7

## Resolución de 8 de mayo de 2024, de la Dirección General de Racionalización y Centralización de la Contratación, en relación a la declaración de contratación centralizada de determinados suministros y servicios

Ministerio de Hacienda
«BOE» núm. 120, de 17 de mayo de 2024
Última modificación: sin modificaciones
Referencia: BOE-A-2024-9980

La Orden EHA/1049/2008, de 10 de abril, de declaración de bienes y servicios de contratación centralizada, en su redacción dada por la Orden HFP/457/2018, de 30 de abril, establece, en su disposición adicional segunda, un régimen de coordinación de la vigencia de determinados contratos que resultan susceptibles de declararse de contratación centralizada de conformidad con lo dispuesto en el artículo 229.1 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

Este régimen responde a la finalidad de garantizar que la aplicación del acuerdo marco, sistema dinámico de adquisición o contrato centralizado no resulte afectada por la vigencia de los contratos de larga duración que, con anterioridad y con el mismo objeto, hubieran podido celebrarse por los distintos Departamentos, organismos y entidades del ámbito subjetivo obligatorio del sistema estatal de contratación centralizada. Para ello, atribuye a la Dirección General de Racionalización y Centralización de la Contratación la competencia para identificar los suministros, obras y servicios susceptibles de ser declarados de contratación centralizada próximamente.

En aplicación de la citada disposición adicional segunda de la Orden EHA/1049/2008, de 10 de abril, se dictó la Resolución de 8 de junio de 2018, de la Dirección General de Racionalización y Centralización de la Contratación, por la que se da cumplimiento a la disposición adicional segunda de la Orden EHA/1049/2008, de 10 de abril, de declaración de bienes y servicios de contratación centralizada (BOE de 13 de junio de 2018).

Analizados los servicios y suministros identificados en la Resolución de 8 de junio de 2018, se hace preciso actualizar aquellos que son susceptibles de ser declarados de contratación centralizada próximamente por la persona titular del Ministerio de Hacienda.

Por ello, examinados los servicios y suministros que se contratan con carácter general y características esencialmente homogéneas por la Administración General del Estado y sus organismos dependientes y, en especial, aquellos cuya contratación centralizada se ha propuesto por entidades incluidas en el ámbito del sistema estatal de contratación centralizada, atendiendo a razones de eficiencia en la gestión de los mismos, así como de planificación de la centralización, en cumplimiento de la disposición adicional segunda de la Orden EHA/1049/2008, de 10 de abril, de declaración de bienes y servicios de contratación

centralizada (BOE de 13 de junio de 2018) esta Dirección General de Racionalización y Centralización de la Contratación acuerda:

**Primero.**

Que los suministros y servicios que se relacionan a continuación resultan susceptibles de ser declarados próximamente de contratación centralizada:

– Combustible para instalaciones, en inmuebles de uso administrativo.
– Gestión de residuos, en inmuebles de uso administrativo.

**Segundo.**

La Administración General del Estado y demás entidades comprendidas en el ámbito subjetivo obligatorio del sistema estatal de contratación centralizada, conforme a lo establecido en el artículo 229.2 de la Ley de Contratos del Sector Público, deberán recabar el informe favorable de la Dirección General de Racionalización y Centralización de la Contratación para tramitar aquellos contratos con duración superior a un año prorrogable por un año adicional, que tengan por objeto los servicios y suministros incluidos en esta Resolución. Asimismo, para acordar la prórroga será necesario informe favorable previo.

**Tercero.**

Dejar sin efecto la Resolución de 8 de junio de 2018, de la Dirección General de Racionalización y Centralización de la Contratación, por la que se da cumplimiento a la disposición adicional segunda de la Orden EHA/1049/2008, de 10 de abril, de declaración de bienes y servicios de contratación centralizada.

**Cuarto.**

Esta Resolución entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado».

# § 8

# Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones

Jefatura del Estado
«BOE» núm. 266, de 5 de noviembre de 2019
Última modificación: sin modificaciones
Referencia: BOE-A-2019-15790

I

La sociedad actual requiere de adaptaciones en la esfera digital que exigen de una traducción en el plano normativo. El desarrollo y empleo de las nuevas tecnologías y redes de comunicaciones por parte de las Administraciones Públicas se está acelerando. Ello exige establecer sin demora un marco jurídico que garantice el interés general y, en particular, la seguridad pública, asegurando la adecuada prestación de los servicios públicos y, al mismo tiempo, que la administración digital se emplee para fines legítimos que no comprometan los derechos y libertades de los ciudadanos.

El carácter estratégico para la seguridad pública de las materias reguladas en este real decreto-ley se ve avalado por la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que describe los riesgos asociados a las nuevas tecnologías como uno de los principales desafíos de la sociedad actual.

La Estrategia de Seguridad Nacional 2017, aprobada mediante Real Decreto 1008/2017, de 1 de diciembre, identifica las ciberamenazas y el espionaje como amenazas que comprometen o socavan la seguridad nacional y, en coherencia con ello, singulariza la ciberseguridad como uno de sus ámbitos prioritarios de actuación. El desarrollo tecnológico implica una mayor exposición a nuevas amenazas, especialmente las asociadas al ciberespacio, tales como el robo de datos e información, el *hackeo* de dispositivos móviles y sistemas industriales, o los ciberataques contra infraestructuras críticas. La hiperconectividad actual agudiza algunas de las vulnerabilidades de la seguridad pública y exige una mejor protección de redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano.

Entre los principales desafíos que las nuevas tecnologías plantean desde el punto de vista de la seguridad pública se encuentran las actividades de desinformación, las interferencias en los procesos de participación política de la ciudadanía y el espionaje. Estas actividades se benefician de las posibilidades que ofrece la sofisticación informática para acceder a ingentes volúmenes de información y datos sensibles.

En este punto juega un papel decisivo el proceso de transformación digital de la Administración, ya muy avanzado. La administración electrónica agudiza la dependencia de las tecnologías de la información y extiende la posible superficie de ataque, incrementando

el riesgo de utilización del ciberespacio para la realización de actividades ilícitas que impactan en la seguridad pública y en la propia privacidad de los ciudadanos.

Los recientes y graves acontecimientos acaecidos en parte del territorio español han puesto de relieve la necesidad de modificar el marco legislativo vigente para hacer frente a la situación. Tales hechos demandan una respuesta inmediata para evitar que se reproduzcan sucesos de esta índole estableciendo un marco preventivo a tal fin, cuyo objetivo último sea proteger los derechos y libertades constitucionalmente reconocidos y garantizar la seguridad pública de todos los ciudadanos.

El presente real decreto-ley tiene por objeto regular este marco normativo, que comprende medidas urgentes relativas a la documentación nacional de identidad; a la identificación electrónica ante las Administraciones Públicas; a los datos que obran en poder de las Administraciones Públicas; a la contratación pública y al sector de las telecomunicaciones.

II

El presente real decreto-ley consta de una parte expositiva y una parte dispositiva estructurada del modo siguiente: capítulo I (artículos 1 y 2), un capítulo II (artículos 3 y 4), un capítulo III (artículo 5), un capítulo IV (artículo 6), un capítulo V (artículo 7), una disposición adicional, tres disposiciones transitorias y tres disposiciones finales.

El capítulo I contempla dos medidas en materia de documentación nacional de identidad, dirigidas a configurar el Documento Nacional de Identidad, con carácter exclusivo y excluyente, como el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular. Con esta finalidad, el artículo 1 del presente real decreto-ley modifica el artículo 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. En coherencia con ello, el artículo 2 del real decreto-ley modifica la regulación del Documento Nacional de Identidad electrónico recogida en el artículo 15.1 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

El capítulo II del presente real decreto-ley, que contiene los artículos 3 y 4, establece varias medidas en materia de identificación electrónica ante las Administraciones Públicas, ubicación de determinadas bases de datos y datos cedidos a otras Administraciones Públicas. La finalidad de estas medidas es garantizar la seguridad pública, tanto en las relaciones entre las distintas Administraciones Públicas cuando traten datos personales, como entre ciudadanos y Administraciones Públicas cuando las últimas proceden a la recopilación, tratamiento y almacenamiento de datos personales en ejercicio de una función pública.

El artículo 3 del presente real decreto-ley modifica los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, a la vez que introduce una nueva disposición adicional sexta a la misma.

La modificación de la letra a) del apartado 2 de los artículos 9 y 10 responde a la necesidad de adaptar sus contenidos al Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, conocido como Reglamento eIDAS, que establece un marco legal común para las identificaciones y firmas electrónicas en la Unión Europea.

La modificación de la letra c) del apartado 2 de los artículos 9 y 10 tiene como finalidad garantizar la seguridad pública en relación con el empleo de sistemas de identificación y firma electrónicas de los interesados cuando se realizan con clave concertada o mediante cualquier otro sistema que cuente con un registro previo como usuario que permita garantizar su identidad y que las Administraciones Públicas consideren válido. Así, en palabras del propio Tribunal Constitucional expresadas en la Sentencia 55/2018, de 24 de mayo, se mantiene la posibilidad de que «cada administración diseñe sus propios sistemas de identificación electrónica o admita los expedidos por otras entidades públicas o privadas y, con ello, que estos sean más o menos complejos según sus preferencias y la relevancia o características del trámite o servicio correspondiente». Ahora bien, para garantizar la seguridad pública, competencia exclusiva del Estado conforme dispone el artículo 1.1 de la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, la modificación efectuada somete a un régimen de autorización previa por parte de la Administración

General del Estado a los sistemas que sean distintos a aquellos del certificado y sello electrónico. Dicha autorización tendrá por objeto, exclusivamente, verificar si el sistema validado tecnológicamente por parte de la Administración u Organismo Público de que se trate puede o no producir afecciones o riesgos a la seguridad pública, de modo que, si así fuera y solo en este caso, la Administración del Estado denegará dicha autorización con base en dichas consideraciones de seguridad pública.

En la misma línea, el nuevo apartado 3, que se añade tanto al artículo 9 como al artículo 10 de la Ley 39/2015, de 1 de octubre, establece la obligatoriedad de que, en relación con los sistemas previstos en la letra c) del apartado 2 de los artículos 9 y 10, los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en territorio español en caso de que se trate de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. Salvo las excepciones que se introducen en la ley, estos datos no podrán ser objeto de transferencia a un tercer país u organización internacional y, en cualquier caso, se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Por último, el artículo 3 del presente real decreto-ley incorpora una disposición adicional sexta a la Ley 39/2015, de 1 de octubre, que prevé que en las relaciones de los interesados con las Administraciones Públicas no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificaciones basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea. Además, la nueva disposición adicional sexta establece que cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal deberá contemplar que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública.

Las restricciones impuestas a los sistemas de identificaciones y firmas basados en tecnologías de registro distribuido en ningún caso suponen una prohibición general. Simplemente, se restringe puntualmente y de forma meramente provisional su uso como sistema de identificación y firma de los interesados cuando estos últimos se interrelacionan con la Administración y mientras no haya más datos o un marco regulatorio *ad hoc* de carácter estatal o europeo que haga frente a las debilidades que implica su uso para los datos y la seguridad pública. La falta de un marco regulatorio *ad hoc* sobre estas nuevas tecnologías justifica que, con carácter urgente y en ejercicio de su competencia para dictar legislación básica, el Estado intervenga sobre la materia con carácter provisional hasta que se avance en el seno de la Unión Europea en el tratamiento de este tipo de tecnologías.

El artículo 4 del presente real decreto-ley procede, por una parte, a la modificación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público introduciendo un nuevo artículo 46 bis, y dando una nueva redacción al artículo 155.

Por una parte, el artículo 46 bis obliga a que, por motivos de seguridad pública, los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, se ubiquen y presten dentro del territorio de la Unión Europea. Asimismo, establece que solo puedan ser cedidos a terceros países cuando estos cumplan con las garantías suficientes que les permitan haber sido objeto de una decisión de adecuación de la Comisión Europea, o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

Por otra parte, la finalidad de la modificación del artículo 155 es permitir un mayor control de los datos cedidos entre Administraciones Públicas, al efecto de garantizar la adecuada utilización de los mismos. Se permite excepcionalmente que la Administración General del Estado pueda adoptar la medida de suspender la transmisión de datos por razones de

seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación.

La licitud del tratamiento de los datos personales para finalidades distintas de las finalidades iniciales viene determinada por la circunstancia de que se trate de finalidades compatibles. Tratándose de finalidades incompatibles, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, prohíbe su tratamiento. No obstante, el propio Reglamento declara ya unas finalidades que estima compatibles: tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. En este sentido, en caso de que el responsable del tratamiento (el cesionario), previo análisis de la compatibilidad de acuerdo con los criterios del artículo 6.4 del citado Reglamento, considere que es compatible, el precepto introduce la obligación adicional de consultar a la administración cedente. La Administración General del Estado podrá oponerse motivadamente y suspender por razones de seguridad nacional.

El capítulo III del presente real decreto-ley regula varias medidas en materia de contratación pública, todas ellas dirigidas a reforzar el cumplimiento de la normativa sobre protección de datos personales y la protección de la seguridad pública en este ámbito.

Los contratistas del sector público manejan en ocasiones, para la ejecución de los respectivos contratos, un ingente volumen de datos personales, cuyo uso inadecuado puede, a su vez, plantear riesgos para la seguridad pública. Por ello, resulta necesario asegurar normativamente su sometimiento a ciertas obligaciones específicas que garanticen tanto el cumplimiento de la normativa en materia de protección de datos personales como la protección de la seguridad pública.

El real decreto-ley modifica la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, con la finalidad de introducir medidas que garanticen en todas las fases de la contratación (expediente de contratación, licitación y ejecución del contrato) el respeto por parte de contratistas y subcontratistas de la legislación de la Unión Europea en materia de protección de datos.

Dichas modificaciones son coherentes con lo previsto en el artículo 6 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, que, respecto de los tratamientos de datos necesarios para el cumplimiento de una obligación legal o de una misión realizada en interés público o en el ejercicio de poderes públicos, permite a los Estados miembros que mantengan o introduzcan disposiciones específicas para fijar los requisitos específicos del tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo.

Así, en primer lugar, el presente real decreto-ley modifica el artículo 35 de la Ley 9/2017, de 8 de noviembre, para incluir, como contenido mínimo de los contratos, la referencia expresa al sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.

En segundo lugar, y por lo que respecta al régimen de invalidez de los contratos, se añade un subapartado al artículo 39.2 de la Ley 9/2017, de 8 de noviembre, para incluir, como causa de nulidad de pleno derecho, la celebración de contratos por parte de poderes adjudicadores que omitan mencionar en los pliegos las obligaciones del futuro contratista en materia de protección de datos a los que se refiere el nuevo artículo 122.2 de la Ley 9/2017, en la redacción dada a dicho precepto por el presente real decreto-ley. La aplicación en este caso de la consecuencia jurídica máxima que contempla nuestro ordenamiento jurídico, esto es, de la nulidad de pleno Derecho, se ha considerado adecuada una vez ponderada la oportunidad de su incorporación en la legislación de contratos del sector público (siguiéndose el dictamen n. 116/2015, del Consejo de Estado), dada la importancia que en determinados casos puede presentar para los intereses de la seguridad nacional conocer la ubicación de los servidores en los que se alojarán los datos que ceda la Administración con motivo de la ejecución de un contrato público, desde dónde se van a prestar los servicios asociados a los mismos y asegurar el sometimiento de la ejecución de ese contrato a la normativa nacional y de la Unión Europea en materia de protección de datos.

En tercer lugar, y en el contexto de la regulación de los requisitos para contratar con el sector público, se modifica el artículo 116.1 de la Ley 9/2017, de 8 de noviembre, para incluir, como circunstancia que impedirá a los empresarios contratar con las entidades comprendidas en el artículo 3 de dicha Ley, el haber dado lugar a la resolución firme de cualquier contrato celebrado con una de tales entidades por incumplimiento culpable de las obligaciones que los pliegos hubieren calificado como esenciales de acuerdo con lo previsto en el art. 211.1.f) de la propia Ley.

En cuarto lugar, se da una nueva redacción al artículo 116.1 de la Ley 9/2017, de 8 de noviembre, introduciendo un segundo párrafo relativo al expediente de contratación de los contratos cuya ejecución requiera de la cesión de datos por parte de entidades del sector público al contratista. En virtud de esta modificación, se incluye la obligación del órgano de contratación de especificar en el expediente cuál será la finalidad de los datos que vayan a ser cedidos.

En quinto lugar, se da una nueva redacción al artículo 122.2 de la Ley 9/2017, de 8 de noviembre, relativo a los pliegos de cláusulas administrativas particulares. En concreto, se añade un párrafo tercero a este apartado para incluir la obligación de los pliegos de mencionar expresamente la obligación del futuro contratista de respetar la normativa vigente en materia de protección de datos. Asimismo, se añade un párrafo cuarto relativo a los contratos que exijan el tratamiento por el contratista de datos personales por parte del responsable del tratamiento, indicando que en estos casos será obligatorio hacer constar en el pliego tanto la finalidad de la cesión de datos como la obligación de la empresa adjudicataria de mantener al contratante al corriente de la ubicación de los correspondientes servidores. También se añade un párrafo quinto para establecer que los extremos mencionados en el párrafo cuarto deben hacerse constar en los pliegos como obligaciones esenciales a los efectos del régimen de resolución del contrato.

En sexto lugar, el presente real decreto-ley da una nueva redacción al artículo 202.1 de la Ley 9/2017, de 8 de noviembre, regulador de las condiciones especiales de ejecución del contrato de carácter social, ético, medioambiental o de otro orden. En concreto, se introduce un párrafo tercero relativo a los pliegos correspondientes a contratos cuya ejecución implique la cesión de datos por las entidades del sector público al contratista. Mediante esta adición se impone la exigencia de que los pliegos incluyan, como condición especial de ejecución, la obligación del contratista de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos. Asimismo, en los pliegos debe advertirse al contratista de que esta obligación tiene el carácter de obligación contractual esencial a los efectos del régimen de resolución del contrato.

En séptimo lugar, el artículo 5 siete del real decreto-ley da una nueva redacción al artículo 215.4 de la Ley 9/2017, relativo a la subcontratación, para incluir, entre las obligaciones del contratista principal, la de asumir la total responsabilidad de la ejecución del contrato frente a la Administración también por lo que respecta a la obligación de sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.

El capítulo IV de este real decreto-ley regula varias medidas para reforzar la seguridad en materia de telecomunicaciones. Así, el artículo 6 de esta norma acomete cinco modificaciones de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, con el objetivo de potenciar las facultades de que dispone el Gobierno, a través del Ministerio de Economía y Empresa, para afrontar situaciones que pueden afectar al mantenimiento del orden público, la seguridad pública o la seguridad nacional.

Así, en concreto, se modifican los artículos 4.6 y 6.3 de la Ley 9/2014, de 9 de mayo, para reforzar las potestades del Ministerio de Economía y Empresa para llevar a cabo un mayor control y para mejorar sus posibilidades de actuación cuando la comisión de una presunta actuación infractora a través del uso de las redes y servicios de comunicaciones electrónicas pueda suponer una amenaza grave e inmediata para el orden público, la seguridad pública o la seguridad nacional o cuando en determinados supuestos excepcionales que también puedan comprometer el orden público, la seguridad pública y la seguridad nacional sea necesaria la asunción de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas.

Estas mayores posibilidades de actuación que se reconocen no se limitan en su aplicación a un concepto estricto de una red o un servicio de comunicaciones electrónicas, sino que extienden su eficacia a los elementos que necesariamente acompañan a la instalación o despliegue de una red o la prestación de un servicio de comunicaciones electrónicas, como son las infraestructuras susceptibles de alojar redes públicas de comunicaciones electrónicas, sus recursos asociados o cualquier elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer el orden público, la seguridad pública y la seguridad nacional.

En necesaria correlación con este reforzamiento de funciones públicas en estas situaciones excepcionales, se potencia igualmente la potestad sancionadora del Ministerio de Economía y Empresa con el objetivo de hacer efectivas y reales las actuaciones que pueda adoptar en uso de estas nuevas facultades de actuación dirigidas a preservar o restablecer el orden público, la seguridad pública y la seguridad nacional. Con esta finalidad, el presente real decreto-ley da una nueva redacción a los artículos 76.15, 77.28 y 81.1 de la Ley 9/2014, de 9 de mayo. En particular, se amplían los supuestos en los que el Ministerio de Economía y Empresa puede adoptar medidas cautelares en casos de razones de imperiosa urgencia sin audiencia previa del presunto infractor, que puede incluir el cese de la actividad o la prestación de servicios, incorporando al efecto algunos de los supuestos que contemplados con dicha finalidad figuran en el artículo 30.6 del Código Europeo de las Comunicaciones Electrónicas, aprobado por la Directiva 2018/1972, de 11 de diciembre de 2018, del Parlamento Europeo y del Consejo, en especial, los relativos a la existencia de una amenaza inmediata y grave para el orden público, la seguridad pública o la seguridad nacional.

Por último, el capítulo V incorpora medidas para reforzar la coordinación en materia de seguridad de las redes y sistemas de información. Para ello, efectúa una modificación del real decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en virtud de la cual el Centro Criptológico Nacional (CCN) ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público. Adicionalmente, se prevé que el CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las Administraciones Públicas con los CSIRT internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad.

III

El real decreto-ley constituye un instrumento constitucionalmente lícito, siempre que el fin que justifica la legislación de urgencia, sea, tal como reiteradamente ha exigido nuestro Tribunal Constitucional (Sentencias 6/1983, de 4 de febrero, F. 5; 11/2002, de 17 de enero, F. 4, 137/2003, de 3 de julio, F. 3 y 189/2005, de 7 julio, F.3), subvenir a un situación concreta, dentro de los objetivos gubernamentales, que por razones difíciles de prever exige una acción normativa inmediata en un plazo más breve que el requerido por la vía normal o por el procedimiento de urgencia para la tramitación parlamentaria de las leyes.

En relación con la concurrencia de los presupuestos habilitantes de extraordinaria y urgente necesidad, debe tenerse en cuenta la doctrina de nuestro Tribunal Constitucional, resumida en el Fundamento Jurídico IV de la Sentencia 61/2018, de 7 de junio de 2018. De acuerdo con ella, se requieren, por un lado, «la presentación explícita y razonada de los motivos que han sido tenidos en cuenta por el Gobierno en su aprobación», es decir, lo que ha venido en denominarse, la situación de urgencia; y, por otro, «la existencia de una necesaria conexión entre la situación de urgencia definida y la medida concreta adoptada para subvenir a ella».

En cuanto a la situación de urgencia, el Tribunal Constitucional ha indicado que «aun habiendo descartado que la utilización por el Gobierno de su potestad legislativa extraordinaria deba circunscribirse a situaciones de fuerza mayor o emergencia, es lo cierto que hemos exigido la concurrencia de ciertas notas de excepcionalidad, gravedad, relevancia e imprevisibilidad que determinen la necesidad de una acción normativa inmediata en un plazo más breve que el requerido para la tramitación parlamentaria de las leyes, bien sea por el procedimiento ordinario o por el de urgencia» (SSTC 68/2007, FJ 10, y

137/2011, FJ 7). También ha señalado el Tribunal Constitucional que la valoración de la extraordinaria y urgente necesidad de una medida puede ser independiente de su imprevisibilidad e, incluso, de que tenga su origen en la previa inactividad del propio Gobierno, siempre que concurra efectivamente la excepcionalidad de la situación, pues «lo que aquí debe importar no es tanto la causa de las circunstancias que justifican la legislación de urgencia cuanto el hecho de que tales circunstancias efectivamente concurran» (STC 11/2002, de 17 de enero, FJ 6).

En cuanto a la conexión de sentido entre la situación de necesidad definida y las medidas que en el real decreto-ley se adoptan, el Tribunal Constitucional atiende a «un doble criterio o perspectiva para valorar la existencia de la conexión de sentido: el contenido, por un lado, y la estructura, por otro, de las disposiciones incluidas en el Real Decreto-ley controvertido» (SSTC 29/1982, de 31 de mayo, FJ 3; 1/2012, de 13 de enero, FJ 11; 39/2013, de 14 de febrero, FJ 9; y 61/2018, de 7 de junio, FJ 4).

La alternativa de introducir estas medidas mediante un proyecto de ley no es factible en el presente caso, habida cuenta de que las Cámaras se encuentran disueltas y no es posible dilatar su adopción hasta la constitución de las Cortes Generales, y, aun utilizándose entonces el trámite de urgencia, no se lograría reaccionar a tiempo.

Los motivos que acaban de exponerse justifican ampliamente la concurrencia de los requisitos constitucionales de extraordinaria y urgente necesidad, que habilitan al Gobierno para aprobar el presente real decreto-ley dentro del margen de apreciación que, en cuanto órgano de dirección política del Estado, le reconoce el artículo 86.1 de la Constitución (STC 142/2014, FJ 3 y STC 61/2018, FFJJ 4 y 7). Concurren también las notas de excepcionalidad, gravedad y relevancia que hacen necesaria una acción normativa inmediata en un plazo más breve que el requerido para la tramitación parlamentaria de una ley, bien sea por el procedimiento ordinario o por el de urgencia (STC 68/2007, FJ 10 y STC 137/2011, FJ 7).

Por lo demás, en el supuesto abordado por este real decreto-ley ha de subrayarse que para subvenir a la situación de extraordinaria y urgente necesidad descrita es necesario proceder a la reforma de varias normas con rango de ley, lo que de por sí exige «una respuesta normativa con rango de ley» (STC 152/2017, de 21 de diciembre, FJ 3 i).

IV

El presente real decreto-ley respeta los límites constitucionalmente establecidos para el uso de este instrumento normativo, pues no afecta al ordenamiento de las instituciones básicas del Estado, a los derechos, deberes y libertades de los ciudadanos regulados en el Título I de la Constitución, al régimen de las comunidades autónomas ni al Derecho electoral general.

Ciertamente, el presente real decreto-ley contiene varias medidas de modificación de leyes preexistentes que refuerzan el cumplimiento de la normativa en materia de protección de datos No obstante, tales normas no constituyen una regulación del régimen general del derecho a la protección de datos, ni van en contra del contenido o elementos esenciales del este derecho, que son los contenidos prohibidos al instrumento jurídico del real decreto-ley según reiterada doctrina constitucional (sintetizada, recientemente, en la STC 139/2016, de 21 julio). Así, el presente real decreto-ley se limita a regular varios aspectos meramente puntuales respecto del tratamiento de datos personales por parte de las Administraciones Públicas y sus contratistas al amparo de la habilitación contenida en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Por lo demás, este real decreto-ley no invade la reserva de ley orgánica prevista en el artículo 81 de la Constitución ni en ningún otro precepto constitucional, en tanto que no se modifican preceptos de carácter orgánico. En particular, carece de carácter orgánico el artículo 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de Protección de la Seguridad Ciudadana, como expresamente dispone la Disposición Final Tercera de dicho texto legal.

V

El artículo 21.3 de la Ley 50/1997, de 27 de noviembre, del Gobierno, habilita al Gobierno en funciones para adoptar medidas distintas al despacho ordinario de los asuntos públicos en «casos de urgencia debidamente acreditados», así como «por razones de interés general cuya acreditación expresa así lo justifique».

Por su parte, los apartados 4 y 5 del artículo 21 de la Ley 50/1997, de 27 de noviembre, recogen una serie de facultades cuyo ejercicio está expresamente vedado al Gobierno en funciones, sin que ninguna de ellas se refiera a la aprobación de reales decretos-leyes. Dichas funciones de ejercicio prohibido para el Ejecutivo en funciones se refieren a cuestiones netamente distintas. En efecto, el artículo 21.4 establece que el Presidente del Gobierno en funciones no podrá proponer al Rey la disolución de alguna de las Cámaras, o de las Cortes Generales, ni plantear la cuestión de confianza, ni tampoco proponer al Rey la convocatoria de un referéndum consultivo. Por su parte, el artículo 21.5 de la Ley 50/1997, de 27 de noviembre, dispone que el Gobierno en funciones no podrá aprobar el Proyecto de Ley de Presupuestos Generales del Estado, ni tampoco presentar proyectos de ley al Congreso de los Diputados o, en su caso, al Senado.

La facultad del Gobierno en funciones de aprobar reales decretos leyes es congruente, por lo demás, con la exigencia de que concurra el presupuesto habilitante de extraordinaria y urgente necesidad previsto en el artículo 86 de la Constitución Española.

VI

El presente real decreto-ley se dicta al amparo de las competencias estatales contempladas en los apartados 18.ª, 21.ª y 29.ª del artículo 149.1 de la Constitución Española.

Por lo que respecta al artículo 149.1.18.ª de la Constitución Española, mediante el presente real decreto-ley se reforman las Leyes 39/2015, de 1 de octubre, y 40/2015, de 1 de octubre, aprobadas por el legislador estatal en ejercicio de su competencia sobre las bases del régimen jurídico de las Administraciones Públicas y sobre el procedimiento administrativo común. Asimismo, el presente real decreto-ley procede a la modificación de varios preceptos de la Ley 9/2017, de 8 de noviembre, preceptos que se enmarcan en la competencia estatal sobre legislación básica en materia de contratos y concesiones administrativas.

En virtud del artículo 149.1.21.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de correos y telecomunicaciones, el presente real decreto-ley modifica varios preceptos de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones y del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

En cuanto a las competencias exclusivas del Estado en materia de seguridad pública (artículo 149.1.29.ª de la Constitución Española), el presente real decreto-ley modifica la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana y el mencionado Real Decreto-ley 12/2018. De acuerdo con este mismo título competencial, se modifica también la Ley 59/2003, de 19 de diciembre, de firma electrónica. Por último, es esta habilitación competencial la que ampara las modificaciones referidas a la necesaria autorización previa por parte de la Administración General del Estado de los sistemas de identificación y firma que cuenten con un registro previo como usuario.

Como se ha justificado en los apartados anteriores, las medidas contenidas en el presente real decreto-ley tienen como finalidad incrementar el estándar de protección de la seguridad pública frente a las crecientes amenazas que plantea el uso de las nuevas tecnologías y a la luz siempre de los últimos sucesos en territorio español. Ha de recordarse que, según la jurisprudencia constitucional, la seguridad pública se refiere a la «actividad dirigida a la protección de personas y bienes (seguridad en sentido estricto) y al mantenimiento de la tranquilidad u orden ciudadanos»; aunque no se limita a regular «las actuaciones específicas de la llamada Policía de seguridad», pues «la actividad policial es una parte de la materia más amplia de la seguridad pública» que «abarca un amplio espectro de actuaciones administrativas» (STC 86/2014, de 29 de mayo, FFJJ 2 y 4, entre otras) e incluye «un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y

contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido» (STC 235/2001, de 13 de diciembre, FJ 6, y las allí citadas).

El Tribunal Constitucional ha situado dentro del concepto de seguridad pública, entre otros extremos, a «las situaciones o productos que son susceptibles de ocasionar graves riesgos para personas y bienes, lo que exige la adopción de medidas de especial intensidad», así como «la regulación de materias concretas susceptibles de originar riesgos ciertos que pueden afectar de modo directo y grave a la seguridad de personas y bienes, tomando en consideración, especialmente, fenómenos colectivos que implican la aparición de amenazas, coacciones o acciones violentas, con graves repercusiones en el funcionamiento de los servicios públicos y en la vida ciudadana» (STC 25/2004, de 26 de febrero, FJ 6).

VII

En la elaboración de este real decreto-ley se han observado los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia, exigidos por el artículo 129 de la Ley 39/2015, de 1 de octubre.

Por una parte, resulta evidente el principio de proporcionalidad, toda vez que las medidas contempladas en esta norma se ajustan plenamente al objetivo que pretende conseguirse mediante este instrumento. Asimismo, cumple los principios de seguridad jurídica ya que es coherente con el resto del ordenamiento jurídico nacional y de la Unión Europea, asegurando su correcta incardinación y congruencia con la regulación vigente. Por lo demás, la norma es coherente con el principio de transparencia al haber cumplido estrictamente con los procedimientos exigidos en la tramitación de un real decreto-ley. No se han realizado los trámites de participación pública, tal y como excepciona para los reales decretos-leyes el artículo 26.11 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

Por otra parte, las medidas contenidas en el real decreto-ley son adecuadas y proporcionadas a las necesidades que exigen su dictado, sin que a estos efectos quepa considerar que existan otras alternativas menos restrictivas o que impongan menos obligaciones a los destinatarios, más bien al contrario, tras la adopción de esta norma con rango de ley se establecerán mejoras sustanciales en el ámbito de la administración electrónica, la contratación pública y las telecomunicaciones.

Se ha solicitado el informe preceptivo de la Oficina de Coordinación y Calidad Normativa, previsto en el artículo 26.9 de la Ley 59/1997, de 27 de noviembre, del Gobierno.

En su virtud, en uso de la autorización concedida en el artículo 86 de la Constitución, a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes e Igualdad, de las Ministras de Justicia, de Defensa, y de Hacienda, del Ministro del Interior, del Ministro de Política Territorial y Función Pública, por suplencia, el Ministro de Agricultura, Pesca y Alimentación, en virtud del Real Decreto 351/2019, de 20 de mayo, y de la Ministra de Economía y Empresa, y previa deliberación del Consejo de Ministros en su reunión del día 31 de octubre de 2019,

DISPONGO:

CAPÍTULO I

**Medidas en materia de documentación nacional de identidad**

**Artículo 1.** *Modificación de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.*

Se modifica el apartado 1 del artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, que queda redactado en los siguientes términos:

«1. Los españoles tienen derecho a que se les expida el Documento Nacional de Identidad.

El Documento Nacional de Identidad es un documento público y oficial y tendrá la protección que a estos otorgan las leyes. Es el único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular.»

**Artículo 2.** *Modificación de la Ley 59/2003, de 19 de diciembre, de firma electrónica.*

Se modifica el apartado 1 del artículo 15 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, en los siguientes términos:

«1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular, en los términos establecidos en el artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, y permite la firma electrónica de documentos.»

CAPÍTULO II

**Medidas en materia de identificación electrónica ante las Administraciones Públicas, ubicación de determinadas bases de datos y datos cedidos a otras Administraciones Públicas**

**Artículo 3.** *Modificación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas queda modificada en los siguientes términos:

Uno. Se modifica el apartado 2 del artículo 9, que queda con el siguiente contenido y se añade un nuevo apartado 3, renumerando el apartado 3 que pasa a ser el apartado 4:

«2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas siguientes:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

c) Sistemas de clave concertada y cualquier otro sistema, que las Administraciones consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c).

3. En relación con los sistemas de identificación previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al

tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4. En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo.»

Dos. Se modifica el apartado 2 del artículo 10, que queda con el siguiente contenido, y se añade un nuevo apartado 3, renumerando los apartados 3 y 4 que pasan a ser 4 y 5:

«2. En el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

c) Cualquier otro sistema que las Administraciones Públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. La autorización habrá de ser emitida en el plazo máximo de tres meses. Sin perjuicio de la obligación de la Administración General del Estado de resolver en plazo, la falta de resolución de la solicitud de autorización se entenderá que tiene efectos desestimatorios.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c).

3. En relación con los sistemas de firma previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4. Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación

contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

5. Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma.»

Tres. Se añade una nueva disposición adicional sexta, con la siguiente redacción:

**«Disposición adicional sexta.** *Sistemas de identificación y firma previstos en los artículos 9.2 c) y 10.2 c).*

1. No obstante lo dispuesto en los artículos 9.2 c) y 10.2 c) de la presente Ley, en las relaciones de los interesados con los sujetos sometidos al ámbito de aplicación de esta Ley, no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea.

2. En todo caso, cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal a que hace referencia el apartado anterior deberá contemplar asimismo que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública.»

**Artículo 4.** *Modificación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.*

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público queda modificada en los siguientes términos:

Uno. Se introduce un nuevo artículo 46 bis, que queda redactado como sigue:

**«Artículo 46 bis.** *Ubicación de los sistemas de información y comunicaciones para el registro de datos.*

Los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, deberán ubicarse y prestarse dentro del territorio de la Unión Europea.

Los datos a que se refiere el apartado anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.»

Dos. Se da nueva redacción al artículo 155, que queda redactado como sigue:

**«Artículo 155.** *Transmisiones de datos entre Administraciones Públicas.*

1. De conformidad con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad.

2. En ningún caso podrá procederse a un tratamiento ulterior de los datos para fines incompatibles con el fin para el cual se recogieron inicialmente los datos personales. De acuerdo con lo previsto en el artículo 5.1.b) del Reglamento (UE) 2016/679, no se considerará incompatible con los fines iniciales el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

3. Fuera del caso previsto en el apartado anterior y siempre que las leyes especiales aplicables a los respectivos tratamientos no prohíban expresamente el tratamiento ulterior de los datos para una finalidad distinta, cuando la Administración Pública cesionaria de los datos pretenda el tratamiento ulterior de los mismos para una finalidad que estime compatible con el fin inicial, deberá comunicarlo previamente a la Administración Pública cedente a los efectos de que esta pueda comprobar dicha compatibilidad. La Administración Pública cedente podrá, en el plazo de diez días oponerse motivadamente. Cuando la Administración cedente sea la Administración General del Estado podrá en este supuesto, excepcionalmente y de forma motivada, suspender la transmisión de datos por razones de seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación. En tanto que la Administración Pública cedente no comunique su decisión a la cesionaria esta no podrá emplear los datos para la nueva finalidad pretendida.

Se exceptúan de lo dispuesto en el párrafo anterior los supuestos en que el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales esté previsto en una norma con rango de ley de conformidad con lo previsto en el artículo 23.1 del Reglamento (UE) 2016/679.»

CAPÍTULO III

**Medidas en materia de contratación pública**

**Artículo 5.** *Modificación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.*

Uno. Se da nueva redacción a la letra d) del apartado 1 del artículo 35, que queda redactado como sigue:

«d) Referencia a la legislación aplicable al contrato, con expresa mención al sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.»

Dos. Se introduce una nueva letra h) al apartado 2 del artículo 39, que queda con la siguiente redacción:

«h) La falta de mención en los pliegos de lo previsto en los párrafos tercero, cuarto y quinto del apartado 2 del artículo 122.»

Tres. Se da nueva redacción a la letra d) del apartado 2 del artículo 71:

«d) Haber dado lugar, por causa de la que hubiesen sido declarados culpables, a la resolución firme de cualquier contrato celebrado con una entidad de las comprendidas en el artículo 3 de la presente Ley. La prohibición alcanzará a las empresas cuyo contrato hubiere quedado resuelto por incumplimiento culpable del contratista de las obligaciones que los pliegos hubieren calificados como esenciales de acuerdo con lo previsto en el artículo 211.1.f).»

Cuatro. Se da nueva redacción al apartado 1 del artículo 116, que queda redactado como sigue:

«1. La celebración de contratos por parte de las Administraciones Públicas requerirá la previa tramitación del correspondiente expediente, que se iniciará por el órgano de contratación motivando la necesidad del contrato en los términos previstos en el artículo 28 de esta Ley y que deberá ser publicado en el perfil de contratante.

En aquellos contratos cuya ejecución requiera de la cesión de datos por parte de entidades del sector público al contratista, el órgano de contratación en todo caso deberá especificar en el expediente de contratación cuál será la finalidad del tratamiento de los datos que vayan a ser cedidos.»

Cinco. Se da nueva redacción al apartado 2 del artículo 122, que queda redactado como sigue:

«2. En los pliegos de cláusulas administrativas particulares se incluirán los criterios de solvencia y adjudicación del contrato; las consideraciones sociales, laborales y ambientales que como criterios de solvencia, de adjudicación o como condiciones especiales de ejecución se establezcan; los pactos y condiciones definidores de los derechos y obligaciones de las partes del contrato; la previsión de cesión del contrato salvo en los casos en que la misma no sea posible de acuerdo con lo establecido en el segundo párrafo del artículo 214.1; la obligación del adjudicatario de cumplir las condiciones salariales de los trabajadores conforme al Convenio Colectivo sectorial de aplicación; y las demás menciones requeridas por esta Ley y sus normas de desarrollo. En el caso de contratos mixtos, se detallará el régimen jurídico aplicable a sus efectos, cumplimiento y extinción, atendiendo a las normas aplicables a las diferentes prestaciones fusionadas en ellos.

Los pliegos podrán también especificar si va a exigirse la transferencia de derechos de propiedad intelectual o industrial, sin perjuicio de lo establecido en el artículo 308 respecto de los contratos de servicios.

Los pliegos deberán mencionar expresamente la obligación del futuro contratista de respetar la normativa vigente en materia de protección de datos.

Sin perjuicio de lo establecido en el artículo 28.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en aquellos contratos cuya ejecución requiera el tratamiento por el contratista de datos personales por cuenta del responsable del tratamiento, adicionalmente en el pliego se hará constar:

a) La finalidad para la cual se cederán dichos datos.

b) La obligación del futuro contratista de someterse en todo caso a la normativa nacional y de la Unión Europea en materia de protección de datos, sin perjuicio de lo establecido en el último párrafo del apartado 1 del artículo 202.

c) La obligación de la empresa adjudicataria de presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos.

d) La obligación de comunicar cualquier cambio que se produzca, a lo largo de la vida del contrato, de la información facilitada en la declaración a que se refiere la letra c) anterior.

e) La obligación de los licitadores de indicar en su oferta, si tienen previsto subcontratar los servidores o los servicios asociados a los mismos, el nombre o el perfil empresarial, definido por referencia a las condiciones de solvencia profesional o técnica, de los subcontratistas a los que se vaya a encomendar su realización.

En los pliegos correspondientes a los contratos a que se refiere el párrafo anterior las obligaciones recogidas en las letras a) a e) anteriores en todo caso deberán ser calificadas como esenciales a los efectos de lo previsto en la letra f) del apartado 1 del artículo 211.»

Seis. Se da nueva redacción al apartado 1 del artículo 202, que queda redactado como sigue:

«1. Los órganos de contratación podrán establecer condiciones especiales en relación con la ejecución del contrato, siempre que estén vinculadas al objeto del contrato, en el sentido del artículo 145, no sean directa o indirectamente

discriminatorias, sean compatibles con el Derecho de la Unión Europea y se indiquen en el anuncio de licitación y en los pliegos.

En todo caso, será obligatorio el establecimiento en el pliego de cláusulas administrativas particulares de al menos una de las condiciones especiales de ejecución de entre las que enumera el apartado siguiente.

Asimismo en los pliegos correspondientes a los contratos cuya ejecución implique la cesión de datos por las entidades del sector público al contratista será obligatorio el establecimiento de una condición especial de ejecución que haga referencia a la obligación del contratista de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos, advirtiéndose además al contratista de que esta obligación tiene el carácter de obligación contractual esencial de conformidad con lo dispuesto en la letra f) del apartado 1 del artículo 211.»

Siete. Se da nueva redacción al apartado 4 del artículo 215, que queda redactado como sigue:

«4. Los subcontratistas quedarán obligados solo ante el contratista principal que asumirá, por tanto, la total responsabilidad de la ejecución del contrato frente a la Administración, con arreglo estricto a los pliegos de cláusulas administrativas particulares o documento descriptivo, y a los términos del contrato; incluido el cumplimiento de las obligaciones en materia medioambiental, social o laboral a que se refiere el artículo 201, así como de la obligación a que hace referencia el último párrafo del apartado 1 del artículo 202 referida al sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos.

El conocimiento que tenga la Administración de los subcontratos celebrados en virtud de las comunicaciones a que se refieren las letras b) y c) del apartado 2 de este artículo, o la autorización que otorgue en el supuesto previsto en la letra d) de dicho apartado, no alterarán la responsabilidad exclusiva del contratista principal.»

## CAPÍTULO IV

## Medidas para reforzar la seguridad en materia de telecomunicaciones

**Artículo 6.** *Modificación de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.*

Uno. Se da nueva redacción al apartado 6 del artículo 4, que queda redactado de la manera siguiente:

«6. El Gobierno, con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de las redes y servicios de comunicaciones electrónicas en determinados supuestos excepcionales que puedan afectar al orden público, la seguridad pública y la seguridad nacional. En concreto, esta facultad excepcional y transitoria de gestión directa o intervención podrá afectar a cualquier infraestructura, recurso asociado o elemento o nivel de la red o del servicio que resulte necesario para preservar o restablecer el orden público, la seguridad pública y la seguridad nacional.

Asimismo, en el caso de incumplimiento de las obligaciones de servicio público a las que se refiere el Título III de esta Ley, el Gobierno, previo informe preceptivo de la Comisión Nacional de los Mercados y de la Competencia, e igualmente con carácter excepcional y transitorio, podrá acordar la asunción por la Administración General del Estado de la gestión directa o la intervención de los correspondientes servicios o de la explotación de las correspondientes redes.

Los acuerdos de asunción de la gestión directa del servicio y de intervención de este o los de intervenir o explotar las redes a los que se refieren los párrafos anteriores se adoptarán por el Gobierno por propia iniciativa o a instancia de una Administración Pública competente. En este último caso, será preciso que la Administración Pública tenga competencias en materia de seguridad o para la prestación de los servicios públicos afectados por el anormal funcionamiento del servicio o de la red de comunicaciones electrónicas. En el supuesto de que el procedimiento se inicie a instancia de una Administración distinta de la del Estado,

aquella tendrá la consideración de interesada y podrá evacuar informe con carácter previo a la resolución final.»

Dos. Se introduce un nuevo apartado 3 en el artículo 6, que queda redactado como sigue:

«3. Las Administraciones Públicas deberán comunicar al Ministerio de Economía y Empresa todo proyecto de instalación o explotación de redes de comunicaciones electrónicas en régimen de autoprestación que haga uso del dominio público, tanto si dicha instalación o explotación vaya a realizarse de manera directa, a través de cualquier entidad o sociedad dependiente de ella o a través de cualquier entidad o sociedad a la que se le haya otorgado una concesión o habilitación al efecto.

El régimen de autoprestación en la instalación o explotación de dicha red puede ser total o parcial, y por tanto dicha comunicación deberá efectuarse aun cuando la capacidad excedentaria de la citada red pueda utilizarse para su explotación por terceros o para la prestación de servicios de comunicaciones electrónicas disponibles al público.

En el caso de que se utilice o esté previsto utilizar, directamente por la administración pública o por terceros, la capacidad excedentaria de estas redes de comunicaciones electrónicas en régimen de autoprestación, el Ministerio de Economía y Empresa verificará el cumplimiento de lo previsto en el artículo 9. A tal efecto, la administración pública deberá proporcionar al Ministerio de Economía y Empresa toda la información que le sea requerida a efecto de verificar dicho cumplimiento.

La obligación establecida en este apartado se entiende sin perjuicio de la prevista en el artículo 7.3 de esta ley.»

Tres. Se da nueva redacción al apartado 15 del artículo 76, que queda redactado como sigue:

«15. El incumplimiento grave de las obligaciones en materia de acceso a redes o infraestructuras físicas susceptibles de alojar redes públicas de comunicaciones electrónicas, interconexión e interoperabilidad de los servicios.»

Cuatro. Se da nueva redacción al apartado 28 del artículo 77, que queda redactado como sigue:

«28. El incumplimiento de las obligaciones en materia de acceso a redes o infraestructuras físicas susceptibles de alojar redes públicas de comunicaciones electrónicas, interconexión e interoperabilidad de los servicios.»

Cinco. Se da nueva redacción al apartado 1 del artículo 81, que queda redactado como sigue:

«1. Previamente al inicio del procedimiento sancionador, podrá ordenarse por el órgano competente del Ministerio de Economía y Empresa, mediante resolución sin audiencia previa, el cese de la presunta actividad infractora cuando existan razones de imperiosa urgencia basada en alguno de los siguientes supuestos:

a) Cuando exista una amenaza inmediata y grave para el orden público, la seguridad pública o la seguridad nacional.

b) Cuando exista una amenaza inmediata y grave para la salud pública.

c) Cuando de la supuesta actividad infractora puedan producirse perjuicios graves al funcionamiento de los servicios de seguridad pública, protección civil y de emergencias.

d) Cuando se interfiera gravemente a otros servicios o redes de comunicaciones electrónicas.

e) Cuando cree graves problemas económicos u operativos a otros proveedores o usuarios de redes o servicios de comunicaciones electrónicas o demás usuarios del espectro radioeléctrico.»

CAPÍTULO V

**Medidas para reforzar la coordinación en materia de seguridad de las redes y sistemas de información**

**Artículo 7.** *Modificación del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.*

Se introduce un apartado 3 en el artículo 11 del siguiente tenor literal:

«3. El Centro Criptológico Nacional (CCN) ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público comprendido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los CSIRT de las Administraciones Públicas consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellos en el ejercicio de sus respectivas funciones.

El CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las Administraciones Públicas con los CSIRT internacionales, en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan.»

**Disposición adicional única.** *Comunicación de las redes de comunicaciones electrónicas en régimen de autoprestación de las Administraciones Públicas.*

Las Administraciones Públicas deberán comunicar al Ministerio de Economía y Empresa en el plazo de un mes de la entrada en vigor de este real decreto-ley las redes de comunicaciones electrónicas en régimen de autoprestación que hagan uso del dominio público a las que se refiere el artículo 6.3 de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones que hayan sido instaladas o estén en proceso de instalación o explotación.

**Disposición transitoria primera.** *Régimen transitorio de las modificaciones introducidas en el artículo 3.*

1. Las entidades del Sector Público que quieran habilitar sistemas de identificación o firma conforme a las letras c) de los artículos 9.2 y 10.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, a partir de la entrada en vigor de este real decreto-ley, deberán solicitar la autorización prevista en dichos preceptos. Los sistemas que, antes de la citada entrada en vigor, ya estén validados y plenamente operativos en los procedimientos administrativos de que se trate, no requerirán someterse a dicha autorización.

2. Las entidades pertenecientes al Sector Público deberán adoptar las medidas necesarias para cumplir la obligación prevista en los artículos 9.3 y 10.3 de la Ley 39/2015, de 1 de octubre, en el plazo máximo de seis meses a partir de la entrada en vigor de este real decreto-ley cuando gestionen directamente o a través de medios propios los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de los sistemas de identificación y firma.

3. En el caso de que la gestión de los recursos citados en el apartado anterior se lleve a cabo mediante la licitación de contratos del Sector Público, directamente por los sujetos a los que es de aplicación la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público o por sus medios propios, la obligación de adaptarse a lo preceptuado en estos artículos no se aplicará a los expedientes de contratación iniciados antes de la entrada en vigor de este real decreto-ley, que se regirán por la normativa anterior. Los contratos adjudicados en virtud de dichos expedientes, aun cuando mantendrán su plena validez y eficacia, no podrán ser objeto de modificación que vulnere lo establecido en los citados preceptos. Tampoco podrán ser objeto de prórroga salvo que previamente sean objeto de modificación para adaptarse a

las disposiciones que en ellos se contienen, siempre y cuando ello sea posible conforme a la Ley 9/2017, de 8 de noviembre.

4. A los efectos de lo dispuesto en esta disposición transitoria se entenderá que los expedientes de contratación han sido iniciados si se hubiera publicado la correspondiente convocatoria del procedimiento de adjudicación del contrato. En el caso de procedimientos negociados sin publicidad, para determinar el momento de iniciación se tomará en cuenta la fecha de aprobación de los pliegos.

5. En el plazo de tres meses desde la entrada en vigor de este real decreto-ley, las distintas Administraciones Públicas remitirán a la Comisión Sectorial de Administración Electrónica la información sobre todos los contratos vigentes que tengan por objeto los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de los sistemas de identificación y firma, así como de aquellos cuyos expedientes ya estén iniciados conforme al apartado anterior.

**Disposición transitoria segunda.** *Régimen transitorio de las modificaciones introducidas en el artículo 4.*

1. Las entidades pertenecientes al Sector Público deberán adoptar las medidas necesarias para cumplir la obligación prevista en el artículo 46 bis de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el plazo máximo de seis meses a partir de la entrada en vigor de este real decreto-ley cuando gestionen directamente o a través de medios propios los sistemas de información y comunicaciones a que dicho precepto se refiere.

2. En el caso de que la gestión de los sistemas citados en el apartado anterior se lleve a cabo mediante la licitación de contratos del Sector Público, directamente por los sujetos a los que es de aplicación la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público o por sus medios propios, la obligación de adaptarse a lo preceptuado en el artículo 46 bis de la Ley 40/2015, de 1 de octubre, no se aplicará a los expedientes de contratación iniciados antes de la entrada en vigor de este real decreto-ley, que se regirán por la normativa anterior.

Los contratos adjudicados en virtud de dichos expedientes, aun cuando mantendrán su plena validez y eficacia, no podrán ser objeto de modificación que vulnere lo establecido en los citados preceptos. Tampoco podrán ser objeto de prórroga salvo que previamente sean objeto de modificación para adaptarse a las disposiciones que en ellos se contienen.

3. A los efectos de lo dispuesto en esta disposición se entenderá que los expedientes de contratación han sido iniciados si se hubiera publicado la correspondiente convocatoria del procedimiento de adjudicación del contrato. En el caso de procedimientos negociados sin publicidad, para determinar el momento de iniciación se tomará en cuenta la fecha de aprobación de los pliegos.

**Disposición transitoria tercera.** *Régimen transitorio de las modificaciones introducidas en el artículo 5.*

1. Los expedientes de contratación iniciados antes de la entrada en vigor de este real decreto-ley se regirán por la normativa anterior. A estos efectos se entenderá que los expedientes de contratación han sido iniciados si se hubiera publicado la correspondiente convocatoria del procedimiento de adjudicación del contrato. En el caso de procedimientos negociados sin publicidad, para determinar el momento de iniciación se tomará en cuenta la fecha de aprobación de los pliegos.

2. No obstante lo anterior, los contratos basados en acuerdos marco que no establezcan todos los términos se regirán por la normativa vigente en la fecha de envío de la invitación a la licitación a las empresas parte del acuerdo marco o por la normativa vigente en la fecha de adjudicación si el contrato basado no requiriera una nueva licitación. En los casos en que el acuerdo marco se hubiera licitado con sujeción a la normativa anterior y, como consecuencia de la aplicación de lo dispuesto en el primer inciso de este párrafo, a alguno o algunos de los contratos basados en ese acuerdo marco le resultara de aplicación la nueva regulación resultante de este Real Decreto-ley, el órgano de contratación deberá elaborar los documentos de la licitación correspondiente a dichos contratos basados de acuerdo con esta nueva regulación.

3. El artículo 5 será de aplicación a las modificaciones de los contratos que se inicien con posterioridad a su entrada en vigor.

**Disposición final primera.** *Títulos competenciales.*

1. Los artículos 1 y 2 de este real decreto-ley se dictan al amparo del artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública.

2. Los artículos 3 y 4, así como las disposiciones transitoria primera y segunda se dictan al amparo del artículo 149.1.18.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva para dictar las bases del régimen jurídico de las Administraciones Públicas y sobre el procedimiento administrativo común y del artículo 149.1.29.ª de la Constitución, que atribuye al Estado competencia exclusiva en materia de seguridad pública.

3. El artículo 5, así como la disposición transitoria tercera, se dictan al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución Española en materia de bases del régimen jurídico de las Administraciones Públicas y en materia de legislación básica sobre contratos y concesiones administrativas y, en consecuencia, son de aplicación general a todas las Administraciones Públicas que entren dentro de su ámbito de aplicación, así como a los organismos y entidades dependientes de ellas.

4. El artículo 6, así como la disposición adicional única, se dictan al amparo de la competencia exclusiva estatal en materia de telecomunicaciones, prevista en el artículo 149.1.21.ª de la Constitución que atribuye al Estado la competencia exclusiva en materia de régimen general de comunicaciones.

5. El artículo 7 se dicta al amparo de las competencias exclusivas atribuidas al Estado en materia de régimen general de telecomunicaciones y seguridad pública, por el artículo 149.1.21.ª de la Constitución, que atribuye al Estado competencia exclusiva en materia de régimen general de comunicaciones y 29.ª de la Constitución, que atribuye al Estado competencia exclusiva en materia de seguridad pública.

**Disposición final segunda.** *Desarrollo reglamentario y ejecución.*

Se habilita al Gobierno y a las personas titulares de los departamentos ministeriales, en el ámbito de sus competencias, a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo dispuesto en este real decreto-ley.

**Disposición final tercera.** *Entrada en vigor.*

El presente real decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

# § 9

# Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social

Ministerio de la Presidencia
«BOE» núm. 279, de 21 de noviembre de 2007
Última modificación: 19 de septiembre de 2018
Referencia: BOE-A-2007-19968

La Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad, contiene una disposición final séptima, que encomienda al Gobierno fijar, en el plazo de dos años desde su entrada en vigor, unas condiciones básicas de accesibilidad y no discriminación para el acceso y utilización de las tecnologías, productos y servicios relacionados con la sociedad de la información y de cualquier medio de comunicación social.

En el mismo sentido, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en su disposición adicional quinta, obliga a las administraciones públicas a adoptar las medidas necesarias para que la información disponible en sus respectivas páginas de internet pueda ser accesible a personas mayores y con discapacidad de acuerdo con los criterios de accesibilidad al contenido generalmente reconocidos, antes del 31 de diciembre de 2005. La disposición adicional quinta establece, asimismo, que las administraciones públicas deben promover la adopción de normas de accesibilidad por parte de los prestadores de servicios y los fabricantes de equipos y de programas de ordenador, para facilitar el acceso de las personas mayores o con discapacidad a los contenidos digitales.

El Consejo de Ministros de 4 de noviembre de 2005 adoptó el Acuerdo por el que se aprueba el Plan 2006-2010 para el desarrollo de la sociedad de la información y de convergencia con Europa y entre comunidades autónomas y ciudades con estatuto de autonomía (Plan Avanza) que incluye un mandato dirigido al Ministerio de Trabajo y Asuntos Sociales, al Ministerio de Industria, Turismo y Comercio y al Ministerio de Administraciones Públicas para que elaboren un proyecto de real decreto por el que se regulen las condiciones de accesibilidad y no discriminación para el acceso y utilización de los servicios relacionados con la sociedad de la información, tomando en consideración, de manera particular, las recomendaciones europeas al respecto.

El presente real decreto se inspira en los principios establecidos en la Ley 51/2003, de 2 de diciembre, fundamentalmente, accesibilidad universal y diseño para todos.

Unos criterios de accesibilidad aplicables a las páginas de Internet son los que se recogen, a nivel internacional, en la Iniciativa de Accesibilidad a la Web (Web Accessibility

Initiative) del Consorcio Mundial de la Web (World Wide Web Consortium), que los ha determinado en forma de pautas comúnmente aceptadas en todas las esferas de internet, como las especificaciones de referencia cuando se trata de hacer que las páginas de Internet sean accesibles a las personas con discapacidad. En función de dichas pautas, la Iniciativa de Accesibilidad a la Web ha determinado tres niveles de accesibilidad: básico, medio y alto, que se conocen como niveles A, AA o doble A y AAA o triple A. Dichas pautas han sido incorporadas en España a través de la Norma UNE 139803:2004, que establece tres niveles de prioridades.

El presente real decreto especifica el grado de accesibilidad aplicable a las páginas de internet de las administraciones públicas, estableciendo como nivel mínimo obligatorio el cumplimiento de las prioridades 1 y 2 de la citada Norma UNE.

En la misma dirección, la Ley 10/2005, de 14 de junio, de medidas urgentes para el impulso de la televisión digital terrestre, de liberalización de la televisión por cable y de fomento del pluralismo, en su disposición adicional 2.ª, se refiere a la garantía de accesibilidad de la televisión digital terrestre para las personas con discapacidad, indicando que las administraciones competentes, previa audiencia a los representantes de los sectores afectados e interesados, adoptarán las medidas necesarias para garantizar desde el inicio la accesibilidad de las personas con discapacidad a los servicios de televisión digital terrestre, concretando que para conseguir este fin, las medidas que se adopten se atendrán a los principios de accesibilidad universal y diseño para todas las personas.

Asimismo, la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en su artículo 3, «Objetivos y principios», contempla la defensa de los intereses y la satisfacción de las necesidades de las personas con necesidades especiales, tales como las personas con discapacidad, y, en su artículo 22, establece, dentro del ámbito del servicio universal, que los usuarios finales con discapacidad deben tener acceso al servicio telefónico disponible al público desde una ubicación fija y a los demás elementos del servicio universal en condiciones equiparables a las que se ofrecen al resto de usuarios finales.

El reglamento de desarrollo de dicha ley, sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por el Real Decreto 424/2005, de 15 de abril, concreta el ámbito del servicio universal, imponiendo obligaciones al operador designado en materia de accesibilidad, como las de garantizar la existencia de una oferta suficiente y tecnológicamente actualizada de terminales especiales adaptados a los diferentes tipos de discapacidades y realizar una difusión suficiente de la misma; la de poner a disposición de todos los usuarios, a través de internet, la guía telefónica en formato accesible; la de poner a disposición de los usuarios ciegos, o con grave discapacidad visual, una determinada franquicia en las llamadas al servicio de consulta telefónica sobre números de abonado, así como la de facilitar, de forma gratuita, las facturas y las condiciones de prestación del servicio, en sistema Braille o en letras grandes; la tarificación especial de las llamadas que se realicen desde cualquier punto del territorio nacional al Centro de Intermediación Telefónica para personas sordas o con discapacidad auditiva y/o de fonación del Ministerio de Trabajo y Asuntos Sociales; la obligación de elaborar planes de adaptación de las cabinas en la vía pública para facilitar su accesibilidad por los usuarios con discapacidad, en particular, por los usuarios ciegos, en silla de ruedas o de talla baja.

Finalmente, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 4.c), establece el principio de accesibilidad a la información y a los servicios por medios electrónicos en los términos establecidos por la normativa vigente en esta materia, a través de sistemas que permitan obtenerlos de manera segura y comprensible, garantizando especialmente la accesibilidad universal y el diseño para todos los soportes, canales y entornos con objeto de que todas las personas puedan ejercer sus derechos en igualdad de condiciones, incorporando las características necesarias para garantizar la accesibilidad de aquellos colectivos que lo requieran.

El presente real decreto, en su disposición adicional primera, amplía las prestaciones que el operador designado ha de ofrecer, modificando el reglamento del servicio universal. En concreto, se incorpora la obligación de que la guía telefónica sea accesible a través de internet con las condiciones de accesibilidad previstas para las páginas web de las administraciones públicas; se amplían las obligaciones relativas a la adaptación de los

teléfonos públicos de pago, de forma que en los citados planes se contemplen expresamente las medidas para facilitar el acceso por usuarios ciegos. Además, dichos planes deberán contemplar la accesibilidad para personas con grave discapacidad visual, tanto de la información visual que se exhiba en el visor del terminal, como de la que figura en la propia cabina. Finalmente, se refuerza la obligación del operador designado en relación con la oferta de terminales fijos adaptados a los distintos tipos de discapacidad y se menciona expresamente la inclusión de soluciones para que las personas con discapacidad visual puedan acceder a los contenidos de las pantallas.

Por otra parte, en el Plan Nacional de Accesibilidad 2004-2012, adoptado por Acuerdo del Consejo de Ministros de 5 de julio de 2003, se pone de relieve que el uso que las personas con discapacidad hacen de las tecnologías, sistemas, productos y servicios relacionados con la comunicación, la información y la señalización es superior al de la media española.

La utilización de los nuevos recursos tecnológicos está muy a menudo vinculada a la calidad de vida, la normalización y la integración en la sociedad de las personas con discapacidad. Por esto, las barreras que se producen en este campo son de especial importancia y han de ser eliminadas de raíz. El presente real decreto se dicta con ese propósito.

El presente real decreto ha sido sometido a consulta de la XXXVI Conferencia Sectorial de Asuntos Sociales, del Consejo Nacional de la Discapacidad, de la Comisión del Mercado de las Telecomunicaciones, del Consejo Asesor de las Telecomunicaciones y para la Sociedad de la Información y del Consejo Superior de Administración Electrónica. Asimismo, ha participado en su elaboración mediante consultas, el tejido social de la discapacidad articulado en torno al Comité Español de Representantes de Personas con Discapacidad.

En su virtud, a propuesta conjunta de los Ministros de Industria, Turismo y Comercio, de Trabajo y Asuntos Sociales y de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de noviembre de 2007,

D I S P O N G O :

**Artículo único.** *Aprobación del Reglamento.*

Se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.

**Disposición adicional primera.** *Modificación del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.*

El Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, se modifica en los siguientes términos:

Uno. Se añade un segundo párrafo al artículo 30.2 en relación con la accesibilidad de la guía telefónica universal a través de internet:

> «El operador designado deberá ofrecer acceso a las guías telefónicas a través de Internet, en formato accesible para usuarios con discapacidad, en las condiciones y plazos de accesibilidad establecidos para las páginas de internet de las administraciones públicas, en el reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.»

Dos. El párrafo segundo del apartado 4 del artículo 32, queda redactado de la siguiente manera:

> «Para ello, el operador designado presentará, para su aprobación por el Ministerio de Industria, Turismo y Comercio, planes de adaptación de los teléfonos públicos de pago para facilitar su accesibilidad por los usuarios con discapacidad y, en particular, por los usuarios ciegos, en silla de ruedas o de talla baja. En relación

con los usuarios ciegos, los planes deberán contemplar la accesibilidad, tanto de la información dinámica facilitada por el visor de terminal, como de la estática a la que se refiere el apartado 3.f) de este artículo. Dichos planes se deberán presentar con un año de antelación a la finalización del que estuviera vigente o cuando el Ministerio de Industria, Turismo y Comercio lo demande por considerar superado el vigente.»

Tres. El párrafo primero del apartado 2 del artículo 33 queda redactado como sigue:

«A los efectos de lo dispuesto en el apartado anterior, el operador designado garantizará la existencia de una oferta suficiente y tecnológicamente actualizada de terminales especiales, adaptados a los diferentes tipos de discapacidades, tales como teléfonos de texto, videoteléfonos o teléfonos con amplificación para personas con discapacidad auditiva, o soluciones para que las personas con discapacidad visual puedan acceder a los contenidos de las pantallas de los terminales, y realizará una difusión suficiente de aquélla.»

Cuatro. El párrafo 2.º del apartado 2.a) del artículo 35, queda redactado del siguiente modo:

«2.º Usuarios ciegos o con grave discapacidad visual. Consistirá en la aplicación de una determinada franquicia en las llamadas al servicio de consulta telefónica sobre números de abonado, y en el establecimiento de las condiciones para la recepción gratuita de las facturas y de la publicidad e información suministrada a los demás abonados de telefonía fija sobre las condiciones de prestación de los servicios, en sistema Braille o en letras o caracteres ampliados, sin menoscabo de la oferta que de esta información se pueda realizar en otros sistemas o formatos alternativos.»

**Disposición adicional segunda.** *Apoyos complementarios.*

De acuerdo con lo ordenado por el artículo 10.2 c) de la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad, se establecen los siguientes apoyos complementarios:

a) Las personas con discapacidad y sus familias podrán beneficiarse de las subvenciones y ayudas económicas que establezcan las administraciones públicas para la adquisición o contratación más ventajosa de elementos, bienes, productos y servicios de la sociedad de la información, en el ámbito de sus competencias.

b) Las personas mayores y con discapacidad tendrán la consideración de grupo de población prioritario en el acceso a las iniciativas, programas y acciones de infoinclusión y de extensión de la sociedad de la información que desarrollen las administraciones públicas. El Ministerio de Trabajo y Asuntos Sociales y el Ministerio de Industria, Turismo y Comercio, a través de los mecanismos adecuados y, en su caso, del Instituto Nacional de Tecnologías de la Comunicación, promoverán el acceso regular y normalizado de las personas con discapacidad a la sociedad de la información.

c) El Centro Estatal de Autonomía Personal y Ayudas Técnicas del Ministerio de Trabajo y Asuntos Sociales y el Ministerio de Industria Turismo y Comercio habilitarán una página de internet, accesible a las personas con discapacidad y mayores, que contendrá información global, completa y actualizada de todos los elementos, bienes, productos y servicios de la sociedad de la información, así como de las iniciativas, programas y acciones que se desarrollen en el ámbito de la sociedad de la información y los medios de comunicación social que tengan relevancia desde la perspectiva de las personas con discapacidad y mayores.

**Disposición adicional tercera.** *Consejo Nacional de la Discapacidad.*

El Consejo Nacional de la Discapacidad, con base en el informe anual o en las medidas o decisiones propuestas por la Oficina Permanente Especializada al Pleno, informará sobre el grado de cumplimiento de las obligaciones en materia de accesibilidad regulada en este real decreto, para ser tenido en cuenta por el departamento ministerial responsable.

**Disposición transitoria única.** *Plazos.*

1. Las obligaciones y medidas contenidas en este real decreto y el reglamento anexo serán exigibles desde el 4 de diciembre de 2009 para todos los productos y servicios nuevos, incluidas las campañas institucionales que se difundan en soporte audiovisual y desde el 4 de diciembre de 2013 para todos aquellos existentes que sean susceptibles de ajustes razonables.

2. Las páginas de internet de las administraciones públicas o con financiación pública deberán adaptarse a lo dispuesto en el artículo 5 de dicho reglamento, en los siguientes plazos:

a) Las páginas nuevas deberán ajustarse a la prioridad 1 de la Norma UNE 139803:2004 desde la entrada en vigor del real decreto.

b) Las páginas existentes deberán adaptarse a la prioridad 1 de la Norma UNE 139803:2004 en el plazo de 6 meses desde la entrada en vigor.

c) Todas las páginas, actualmente existentes o de nueva creación, deberán cumplir la prioridad 2 de la Norma UNE 139803:2004 a partir del 31 de diciembre de 2008. No obstante, este plazo de adaptación y la citada norma técnica de referencia podrán ser modificados a efectos de su actualización mediante orden ministerial conjunta, en los términos establecidos en la disposición final tercera de este real decreto.

3. Las obligaciones que la disposición adicional primera de este real decreto introduce en el reglamento aprobado por el Real Decreto 424/2005, de 15 de abril, deberán ser cumplidas a partir de la entrada en vigor del presente real decreto, a excepción de lo en ella previsto para la accesibilidad a la guía telefónica universal a través de Internet, a la que serán de aplicación los plazos establecidos en el apartado anterior.

**Disposición final primera.** *Financiación.*

Las medidas previstas en el presente real decreto, serán financiadas con cargo a los créditos ordinarios de los correspondientes departamentos y organismos públicos competentes.

**Disposición final segunda.** *Título competencial.*

1. Este real decreto se dicta al amparo de las reglas 1.ª y 21.ª del artículo 149.1 de la Constitución, que reservan al Estado, respectivamente, competencias para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales y en materia de telecomunicaciones.

2. Los artículos 5 y 8 del reglamento anexo al presente real decreto tienen el carácter de legislación básica sobre el régimen jurídico de las administraciones públicas, de conformidad con lo dispuesto en el artículo 149.1.18.ª de la Constitución.

**Disposición final tercera.** *Facultades de desarrollo.*

Se autoriza a los Ministros de Economía y Hacienda, de Trabajo y Asuntos Sociales, de Industria, Turismo y Comercio y de Administraciones Públicas, previa consulta al Consejo Nacional de la Discapacidad y al sector de operadores y empresas obligadas a cumplir las medidas del real decreto, a proponer al Ministro de la Presidencia la adopción mediante orden de cuantas disposiciones sean necesarias para la actualización de estándares determinados en el reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social o el reconocimiento de otros nuevos.

**Disposición final cuarta.** *Accesibilidad de páginas de internet.*

En al ámbito de la Administración General del Estado, la excepcionalidad prevista en el artículo 5.2 del Reglamento, se determinará por Orden de la Ministra de la Presidencia dictada a propuesta conjunta de los Ministros de Economía y Hacienda, de Trabajo y

Asuntos Sociales, de Industria, Turismo y Comercio y de la Ministra de Administraciones Públicas.

**Disposición final quinta.** *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## REGLAMENTO SOBRE LAS CONDICIONES BÁSICAS PARA EL ACCESO DE LAS PERSONAS CON DISCAPACIDAD A LAS TECNOLOGÍAS, PRODUCTOS Y SERVICIOS RELACIONADOS CON LA SOCIEDAD DE LA INFORMACIÓN Y MEDIOS DE COMUNICACIÓN SOCIAL

### CAPÍTULO I

### Disposiciones generales

**Artículo 1.** *Objeto del reglamento.*

El objeto de este reglamento es establecer los criterios y las condiciones que se consideran básicos para garantizar el acceso de las personas con discapacidad a las tecnologías, productos y servicios de la sociedad de la información y de cualquier medio de comunicación social, de acuerdo con los principios de igualdad de oportunidades, no discriminación y accesibilidad universal.

**Artículo 2.** *Ámbito de aplicación.*

Las administraciones públicas, los operadores de telecomunicaciones, los prestadores de servicios de la sociedad de la información y los titulares de medios de comunicación social que presten sus servicios bajo la jurisdicción española deberán cumplir las condiciones básicas de accesibilidad que se establecen en el presente reglamento.

### CAPÍTULO II

### Condiciones básicas de accesibilidad y no discriminación en materia de telecomunicaciones

**Artículo 3.** *Condiciones básicas de accesibilidad a los servicios de atención al cliente y al contenido de los contratos, facturas y demás información exigida.*

1. Los operadores deberán realizar los ajustes razonables que permitan el acceso por las personas con discapacidad al servicio de atención al cliente, referido en el artículo 104 del reglamento, aprobado por el Real Decreto 424/2005, de 15 de abril, en los plazos establecidos en la disposición final séptima de la Ley 51/2003, de 2 de diciembre.

2. Asimismo, los operadores deberán facilitar a los abonados con discapacidad visual que lo soliciten, en condiciones y formatos accesibles, los contratos, facturas, y demás información suministrada a todos los abonados en cumplimiento de lo dispuesto en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y su normativa de desarrollo, en materia de derechos de los usuarios. Cuando la información o comunicación se realice a través de internet, será de aplicación lo dispuesto en este reglamento para las páginas de las administraciones públicas o con financiación pública.

**Artículo 4.** *Condiciones básicas de accesibilidad al servicio de telefonía móvil.*

1. Sin perjuicio de lo dispuesto en el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por el Real Decreto 424/2005, de 15 de abril, el Ministerio de Trabajo y Asuntos Sociales, a través del Centro Estatal de Autonomía Personal y Ayudas Técnicas, promoverá la existencia de una oferta suficiente y tecnológicamente actualizada de terminales de telefonía móvil especiales, adaptados a los diferentes tipos de

discapacidades. A estos efectos, se tendrán en consideración, entre otros, los siguientes elementos o facilidades:

a) Marcación vocal y gestión de las funciones principales del teléfono por voz.

b) Información, a través de una síntesis de voz, de las diferentes opciones disponibles en cada momento o de cualquier cambio que se produzca en la pantalla.

c) Generación de voz para facilitar la accesibilidad de los SMS.

d) Conectores para instalar equipos auxiliares tales como auriculares, amplificadores con bobina inductiva, pantallas externas, o teclados para enviar mensajes.

e) Pantallas de alto contraste, con caracteres grandes o ampliados y posibilidad de configuración por el usuario.

2. Cuando, de acuerdo con la Directiva 1999/5/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicaciones y reconocimiento mutuo de su conformidad, la Comisión Europea decida la incorporación de requisitos adicionales en los equipos terminales de telefonía móvil, relativos a la compatibilidad de los mismos con las funcionalidades que faciliten su utilización por usuarios con discapacidad, su publicación en España se hará mediante resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, de acuerdo con lo dispuesto en el artículo 4 del Reglamento que establece el procedimiento para la evaluación de la conformidad de los aparatos de telecomunicaciones, aprobado por el Real Decreto 1890/2000, de 20 de noviembre.

## CAPÍTULO III

## Criterios y condiciones básicas de accesibilidad y no discriminación en materia de sociedad de la información

**Artículo 5.** *Criterios de accesibilidad aplicables a las páginas de internet de las administraciones públicas o con financiación pública.*

**(Derogado).**

**Artículo 6.** *Criterios de accesibilidad a otras páginas de internet.*

**(Derogado).**

**Artículo 7.** *Sistema de certificación de páginas de internet.*

**(Derogado).**

**Artículo 8.** *Condiciones básicas de accesibilidad a los equipos informáticos y a los programas de ordenador.*

1. Los equipos informáticos y los programas de ordenador -independientemente de que sea libre o esté sometido a derechos de patente o al pago de derechos-utilizados por las administraciones públicas, cuyo destino sea el uso por el público en general, deberán ser accesibles a las personas mayores y personas con discapacidad, de acuerdo con el principio rector de «Diseño para todos» y los requisitos concretos de accesibilidad exigidos, preferentemente en las normas técnicas nacionales que incorporen normas europeas, normas internacionales, otros sistemas de referencias técnicas elaborados por los organismos europeos de normalización o, en su defecto, normas nacionales (Normas UNE 139801:2003 y 139802:2003), y en los plazos establecidos en el apartado 1 de la disposición transitoria única del real decreto por el que se aprueba el presente reglamento.

2. Se deberán promover medidas de sensibilización y difusión para que los fabricantes de equipos informáticos y de programas de ordenador incorporen a sus productos y servicios, progresivamente y en la medida de lo posible, los criterios de accesibilidad y de «Diseño para todos», que faciliten el acceso de las personas mayores y personas con discapacidad a la sociedad de la información.

**Artículo 9.** *Condiciones básicas de accesibilidad en servicios y productos de confianza.*

Los servicios de confianza prestados y los productos para las personas usuarias finales utilizados en la prestación de estos servicios deberán ser accesibles para las personas mayores y personas con discapacidad. Excepcionalmente, esta obligación no será aplicable cuando el producto o servicio de confianza no disponga de una solución tecnológica que permita su accesibilidad.

CAPÍTULO IV

**Condiciones básicas de accesibilidad y no discriminación en materia de medios de comunicación social**

**Artículo 10.** *Condiciones básicas de accesibilidad a los contenidos de la televisión.*

1. Las personas con discapacidad tendrán acceso a los contenidos de los medios de comunicación audiovisual, con arreglo a las disponibilidades que permite el progreso técnico, los diseños universales y los ajustes razonables que, para atender las singularidades que presentan estas personas, sea preciso llevar a cabo.

2. Los contenidos audiovisuales de la televisión serán accesibles a las personas con discapacidad mediante la incorporación de la subtitulación, la audiodescripción y la interpretación en lengua de signos, en los términos establecidos específicamente en la legislación general audiovisual, que regulará, con carácter de norma básica, las condiciones de acceso y no discriminación en los contenidos de la televisión.

**Artículo 11.** *Condiciones básicas de accesibilidad a la televisión digital.*

1. Las administraciones públicas adoptarán las medidas necesarias para garantizar el acceso de las personas con discapacidad a los servicios de televisión digital, de acuerdo con los principios de accesibilidad universal y diseño para todas las personas.

2. Las administraciones públicas adoptarán las medidas necesarias para garantizar a las personas con discapacidad la existencia de una oferta suficiente de equipos receptores de televisión digital que permitan recibir sus contenidos, faciliten la navegación a través de los menús de configuración, las guías electrónicas de programación, los servicios interactivos y otros contenidos textuales, así como todas las prestaciones básicas que ofrecen los receptores de televisión digital, de acuerdo con los principios de accesibilidad universal y de diseño para todos.

Las herramientas de accesibilidad, que a tal efecto se utilicen, podrán integrar los siguientes elementos tecnológicos:

a) Conversión de texto a voz para favorecer la navegabilidad de los menús de configuración, las guías electrónicas de programación y los servicios interactivos y otros contenidos textuales.

b) Aplicaciones de reconocimiento de voz para efectuar operaciones de configuración, de solicitud de información de las guías electrónicas de programación o empleo de servicios interactivos u otros contenidos textuales.

c) Ergonomía en los receptores de televisión digital, así como en todos sus dispositivos asociados, y, muy especialmente, en el diseño de los mandos a distancia.

d) Aplicaciones de personalización para que, personas con discapacidad puedan configurar los receptores de televisión digital, y, muy particularmente, los parámetros de visualización: tamaño y color de la fuente de letras, color de fondo, contraste y otros.

e) Otras herramientas técnicas diseñadas para hacer accesibles los contenidos recibidos a través de la televisión digital a las personas con discapacidad, facilitando el manejo del receptor y permitiendo una recepción de la televisión digital sin barreras y adecuada al tipo y grado de discapacidad.

Las administraciones públicas, en la esfera de sus respectivas competencias, fomentarán la difusión pública de las medidas de accesibilidad a la televisión digital, coordinarán actuaciones y sinergias entre todos los agentes implicados, y desarrollarán planes de investigación, desarrollo e innovación (I+D+i), a fin de favorecer la implantación y la puesta en práctica de las tecnologías necesarias para que las personas con discapacidad

tengan pleno acceso a la televisión digital. Igualmente, las administraciones públicas implicadas, promoverán el desarrollo de políticas de normalización, códigos de buenas prácticas y herramientas que incorporen requisitos de accesibilidad.

**Artículo 12.** *Condiciones básicas de accesibilidad de la publicidad institucional en soporte audiovisual.*

1. De conformidad con lo dispuesto en la Ley 29/2005, de 29 de diciembre, de publicidad y comunicación institucional, aquellas campañas institucionales que se difundan en soporte audiovisual, preverán siempre en sus pliegos de cláusulas los procedimientos de acondicionamiento destinados a permitir que los mensajes contenidos sean accesibles para las personas con discapacidad y edad avanzada.

2. A los efectos de este artículo, la accesibilidad comprenderá la subtitulación en abierto de los mensajes hablados. Para la emisión en lengua de signos de los mensajes hablados (sistema de ventana menor en ángulo de la pantalla), la audiodescripción y la locución de todos los mensajes escritos que aparezcan, se estará a lo regulado por la Ley 27/2007, de 23 de octubre, por la que se reconocen las lenguas de signos españolas y se regulan los medios de apoyo a la comunicación oral de las personas sordas, con discapacidad auditiva y sordociegas. Todos estos procedimientos de acondicionamiento para permitir la accesibilidad se realizarán con arreglo a las normas técnicas establecidas para cada caso.

3. El presente artículo será de aplicación exclusiva en el ámbito de la Administración General del Estado y las demás entidades integrantes del sector público estatal.

# § 10

## Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público

Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad
«BOE» núm. 227, de 19 de septiembre de 2018
Última modificación: 12 de agosto de 2019
Referencia: BOE-A-2018-12699

La Directiva (UE) 2016/2102, del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público tiene como objeto, a fin de mejorar el funcionamiento del mercado interior, aproximar las disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a los requisitos de accesibilidad, entendiendo la accesibilidad como un conjunto de principios y técnicas que se deben respetar a la hora de diseñar, construir, mantener y actualizar los sitios web y las aplicaciones para dispositivos móviles.

La Directiva cubre todos los sitios web y aplicaciones móviles del sector público, desde los de la Administración estatal, Administraciones regionales y locales, Tribunales y órganos constitucionales a los de los servicios gestionados por éstas como Hospitales, Colegios, Universidades, Bibliotecas públicas, etc.

En este contexto, la Directiva exige que los sitios web y las aplicaciones para dispositivos móviles de los organismos del sector público se basen en requisitos comunes de accesibilidad establecidos a nivel europeo, poniendo fin a la fragmentación del mercado y a la diferenciación técnica hoy existente, evitando que los países apliquen diferentes versiones, niveles de cumplimiento o tengan diferencias técnicas a escala nacional, reduciendo la incertidumbre de los desarrolladores y fomentando la interoperabilidad. Aspectos todos, que deberían redundar en un aumento del potencial mercado interior de los productos y servicios relacionados con la accesibilidad de sitios web y aplicaciones para dispositivos móviles y por ende, contribuir al crecimiento económico y a la creación de empleo en la Unión Europea.

Para la consecución de este objetivo y asegurar que los ciudadanos se beneficien de un acceso más amplio a los servicios del sector público mediante sitios web y aplicaciones para dispositivos móviles cada vez más accesibles, la Directiva establece unos requisitos mínimos de accesibilidad obligatorios y adopta normas aplicables al diseño, construcción, mantenimiento y actualización de tales sitios web y aplicaciones para dispositivos móviles. A su vez, se impone la elaboración, actualización periódica y publicación de una declaración de accesibilidad sobre la conformidad de sus sitios web y aplicaciones para dispositivos móviles con los requisitos mínimos de accesibilidad que estén establecidos, facilitando la adaptación al estado de la técnica en cada momento. No obstante, la Directiva contempla excepciones al cumplimiento de estos requisitos cuando supongan una carga

desproporcionada para el organismo, sin que en ningún caso la falta de prioridad, tiempo o conocimientos puedan ser considerados como motivos legítimos para la excepción.

Por otro lado, para garantizar el cumplimiento de las previsiones establecidas en esta directiva se exige a cada Estado miembro la creación de un mecanismo de comunicación vinculado a un procedimiento de aplicación que permita, a cualquier persona usuaria de un sitio web o una aplicación para dispositivos móviles de un organismo del sector público, informar de la existencia de incumplimientos de los requisitos de accesibilidad, formular quejas y plantear sugerencias. Así como el establecimiento de un órgano, responsable del procedimiento de aplicación, que garantice que las comunicaciones y solicitudes recibidas se tratan de forma efectiva.

Asimismo, la Directiva (UE) 2016/2102, de 26 de octubre de 2016, impone a los Estados miembros la obligación de establecer un sistema de seguimiento y presentación de informes periódicos a la Comisión Europea, la adopción de medidas de promoción, formación y concienciación en materia de accesibilidad de todos los implicados y responsables jerárquicos y por último, invita a los Estados miembros a ampliar el ámbito de aplicación de sus normas a otros tipos de sitios web y de aplicaciones para dispositivos móviles.

Desde el punto de vista normativo la necesidad de regular unas condiciones básicas de accesibilidad para la utilización de servicios relacionados con la sociedad de la información se reconoce por primera vez en nuestro ordenamiento interno en la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad, que fijaba al Gobierno un plazo de dos años para su establecimiento. Los preceptos de dicha ley, actualmente derogada, se encuentran incluidos en el Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el texto refundido de la Ley General de las personas con discapacidad y de su inclusión social.

Posteriormente, el 4 de diciembre de 2005, el Consejo de Ministros adoptó mediante Acuerdo el Plan 2006-2010 para el desarrollo de la sociedad de la información y de convergencia con Europa y entre comunidades autónomas y ciudades con Estatuto de autonomía (Plan Avanza), que incluía un mandato dirigido a los entonces Ministerio de Trabajo y Asuntos Sociales, al Ministerio de Industria, Turismo y Comercio y al Ministerio de Administraciones Públicas para que elaborasen un proyecto de real decreto que regulase dichas condiciones básicas. Fruto de este mandato es el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social, aprobado por el Real Decreto 1494/2007, de 12 de noviembre, que incluye en su capítulo III medidas específicas en materia de accesibilidad para las páginas de Internet de las Administraciones Públicas o entidades con financiación pública.

También existen otras normas que hacen referencia a los requisitos de accesibilidad de los sitios web de las Administraciones Públicas para las cuáles este nuevo real decreto asentará las bases. Algunas de ellas son la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, la Ley 27/2007, de 23 de octubre, por la que se reconocen las lenguas de signos españolas y se regulan los medios de apoyo a la comunicación oral de las personas sordas, con discapacidad auditiva y sordociegas, y la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. Este real decreto viene a complementar al Real Decreto 1494/2007, de 12 de noviembre, y para ello deroga los artículos del reglamento que hacen referencia a la accesibilidad de las páginas de internet, los artículos 5, 6 y 7, y los desarrolla con mayor detalle. Por lo tanto, este Reglamento recoge los aspectos relativos a los requisitos mínimos de accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público, adoptando las medidas necesarias para cumplir con las disposiciones de la Directiva (UE) 2016/2102, de 26 de octubre de 2016, y, de este modo, seguir garantizando que la accesibilidad y no discriminación, en general y especialmente de las personas con discapacidad en sus relaciones con el sector público, sean reales y efectivas. A tal efecto, además de establecer

los requisitos mínimos que deben cumplirse e incorporar el resto de actuaciones previstas en la Directiva, este real decreto establece el sistema a través del cual las personas usuarias podrán comunicar al organismo del sector público cualquier posible incumplimiento por parte de su sitio web o de su aplicación para dispositivos móviles de los requisitos de accesibilidad establecidos y que también permita solicitar a las personas interesadas, previa solicitud razonable y legítima, la información sobre contenidos que están excluidos del ámbito de aplicación de este real decreto o exentos del cumplimiento de los requisitos de accesibilidad por imponer una carga desproporcionada.

La posibilidad de acudir al Defensor del Pueblo como propone la Directiva en su artículo 9, ya está recogida en la regulación española actual y se refleja en la Ley Orgánica 3/1981, de 6 de abril, del Defensor del Pueblo, que prevé la posibilidad de interponer quejas ante el Defensor del Pueblo para la defensa de los derechos del título I de la Constitución Española, y referidas al funcionamiento de la Administración, lo que incluye las actuaciones de todo el sector público en materia de accesibilidad con el nivel de obligaciones que imponga en cada momento la regulación vigente.

También existe la Oficina de Atención a la Discapacidad de acuerdo con lo previsto en el texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013, de 29 de noviembre. Dicha Oficina es el órgano del Consejo Nacional de la Discapacidad, de carácter permanente y especializado, encargado de promover la igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y realiza las funciones de asesoramiento, análisis y estudio de las quejas, denuncias y consultas presentadas por las personas con discapacidad en los ámbitos de las telecomunicaciones y de la sociedad de la información, entre otras.

Por otro lado, este real decreto también incorpora, en una disposición adicional, los requisitos impuestos a las páginas de Internet de entidades, empresas y centros que prestan servicios públicos a través de una concesión pública, o alguna otra vía contractual con la Administración.

Asimismo, y también en una disposición adicional, se establecen los criterios de accesibilidad aplicables a los sitios web y aplicaciones para dispositivos móviles de los órganos constitucionales del Estado y de los órganos legislativos y de control autonómicos, mediante la adecuación de su normativa específica a lo establecido en este real decreto, y siempre, de acuerdo con lo establecido en la misma.

Con respecto a su entrada en vigor, la Directiva da flexibilidad a los Estados Miembros exigiendo que como mínimo se apliquen todas las previsiones para sitios web nuevos antes del 23 de septiembre de 2019 y para todos los sitios web antes del 23 de septiembre de 2020. Considerando que en España se parte de una legislación existente en la que para sitos web ya se estaban exigiendo gran parte de estos requisitos, se ha diseñado la entrada en vigor de este real decreto dando continuidad a las previsiones del Real Decreto 1494/2007, de 12 de noviembre. De este modo, en el contexto español, se ha optado por una introducción escalonada en los mismos términos que la Directiva únicamente para los aspectos relacionados con la gestión de las quejas y reclamaciones y las aplicaciones móviles. También, atendiendo a las solicitudes recibidas desde el sector de las personas con discapacidad se han adelantado algunos de los plazos previstos en la Directiva. En cualquier caso, las previsiones de este real decreto se han adaptado temporalmente para hacer posible dar respuesta en tiempo y forma a la Comisión Europea con respecto al seguimiento y presentación de informes. El presente real decreto tiene carácter de legislación básica al amparo de lo dispuesto en el artículo 149.1.1.ª y 18.ª de la Constitución Española.

En la elaboración de este real decreto se han recabado los informes del Consejo Territorial de Servicios Sociales y del Sistema para la Autonomía y Atención a la Dependencia, del Consejo Estatal de las Personas Mayores, del Consejo Nacional de la Discapacidad, en el que tienen representación las organizaciones representativas de personas con discapacidad, del Consejo de Consumidores y Usuarios, del Consejo Estatal de Organizaciones no Gubernamentales de Acción Social, de la Comisión Sectorial de Administración Electrónica de la Conferencia Sectorial de Administración Pública, de la

Comisión de Estrategia TIC de la Administración General del Estado y del Comité Técnico Estatal de la Administración Judicial Electrónica.

El presente real decreto, que con arreglo al artículo 25 de la Ley 50/1997, de 27 de noviembre, del Gobierno, está incluido en el Plan Anual Normativo de 2018, asume el mandato de transposición de la Directiva (UE) 2016/2102, de 26 de octubre de 2016. La transposición se ha basado en los principios de la buena regulación previstos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En particular, se ajusta al principio de necesidad y eficacia al cumplir la obligación de incorporación al derecho nacional con fidelidad al texto de la directiva; así como a los principios de proporcionalidad, al contener la regulación imprescindible para el fin que se persigue, transparencia, en la medida en que refuerza las garantías que lo rodean y favorece su cumplimiento, así como de seguridad jurídica, puesto que se realiza con el fin de mantener un marco normativo estable, predecible, integrado y claro.

En su virtud, a propuesta de la Ministra de Política Territorial y Función Pública, de la Ministra de Economía y Empresa y de la Ministra de Sanidad, Consumo y Bienestar Social, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 7 de septiembre de 2018,

DISPONGO:

CAPÍTULO I

**Disposiciones generales**

**Artículo 1.** *Objeto.*

1. Este real decreto tiene por objeto garantizar los requisitos de accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público y otros obligados incluidos en el ámbito de aplicación del artículo 2.

2. A los efectos de este real decreto se entiende por accesibilidad el conjunto de principios y técnicas que se deben respetar al diseñar, construir, mantener y actualizar los sitios web y las aplicaciones para dispositivos móviles para garantizar la igualdad y la no discriminación en el acceso de las personas usuarias, en particular de las personas con discapacidad y de las personas mayores.

**Artículo 2.** *Ámbito subjetivo.*

1. Este real decreto se aplica al sector público que comprende:

a) La Administración General del Estado.
b) Las Administraciones de las comunidades autónomas.
c) Las entidades que integran la Administración Local.
d) El sector público institucional, en los términos establecidos en el artículo 2.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones públicas
e) Las asociaciones constituidas por las Administraciones, entes, organismos y entidades que integran el sector público.

2. Lo dispuesto en este real decreto también será de aplicación a la Administración de Justicia.

**Artículo 3.** *Ámbito objetivo de aplicación.*

1. Este real decreto se aplica tanto a los sitios web, independientemente del dispositivo empleado para acceder a ellos, como a las aplicaciones para dispositivos móviles de los organismos del sector público y otros obligados incluidos en el ámbito de aplicación del artículo 2.

2. El contenido accesible de los sitios web y de las aplicaciones para dispositivos móviles incluye la información tanto textual como no textual, los documentos y formularios que se

pueden descargar, los contenidos multimedia pregrabados de base temporal, las formas de interacción bidireccional, el tratamiento de formularios digitales y la cumplimentación de los procesos de identificación, autenticación, firma y pago con independencia de la plataforma tecnológica que se use para su puesta a disposición del público.

3. Están excluidos de este real decreto y se regularán por su normativa específica los contenidos multimedia en directo y pregrabado de base temporal de los sitios web y aplicaciones para dispositivos móviles de prestadores del servicio público de radiodifusión y sus filiales, así como los de otros organismos o sus filiales que cumplan un mandato de servicio público de radiodifusión.

4. Asimismo, quedan excluidos del ámbito de aplicación del presente real decreto los siguientes contenidos:

a) Formatos de archivo de ofimática publicados antes de la entrada en vigor de este real decreto, salvo que los mismos sean necesarios para tareas administrativas activas relativas a las funciones realizadas por los sujetos obligados por este real decreto.

b) Contenido multimedia pregrabado de base temporal publicado antes de la entrada en vigor de este real decreto.

c) Contenido multimedia en directo de base temporal salvo lo dispuesto en otra legislación específica que obligue al respecto.

d) Servicios de mapas y cartografía en línea, siempre y cuando la información esencial se proporcione de manera accesible digitalmente en el caso de mapas destinados a fines de navegación.

e) Contenidos de terceros que no estén financiados ni desarrollados por el sujeto obligado ni estén bajo su control.

f) Reproducciones de bienes de colecciones del patrimonio que no puedan hacerse plenamente accesibles por alguna de las siguientes causas:

1.° Incompatibilidad de los requisitos de accesibilidad con la conservación del bien de que se trate o con la autenticidad de la reproducción.

2.° Indisponibilidad de soluciones automatizadas y rentables que permitan extraer el texto de manuscritos u otros bienes de colecciones del patrimonio y transformarlos en contenidos compatibles con los requisitos de accesibilidad.

g) Contenidos de extranet e intranet entendidos como sitios web accesibles únicamente para un grupo restringido de personas y no para el público en general, publicados antes del 23 de septiembre de 2019, hasta que dichos sitios web sean objeto de una revisión sustancial.

h) Contenidos de sitios web y aplicaciones para dispositivos móviles que tengan la condición de archivos o herramientas de archivo por contener únicamente contenidos no necesarios para el desarrollo de cualesquiera tareas administrativas activas, siempre que no hayan sido actualizados ni editados con posterioridad a la entrada en vigor de este real decreto.

**Artículo 4.** *Definiciones.*

A efectos del presente real decreto se entiende por:

a) Sitio web: Es un conjunto de archivos electrónicos y páginas web referentes a un tema en particular bajo un nombre de dominio específico a los que se accede utilizando un navegador web.

b) Aplicaciones para dispositivos móviles: Son las aplicaciones informáticas diseñadas y desarrolladas para ser usadas por el público en general en dispositivos móviles, entre los que se incluyen los teléfonos inteligentes y las tabletas. No incluyen el programa «software» que controla dichos dispositivos (sistemas operativos para dispositivos móviles) ni el equipo informático.

c) Archivo ofimático: Son los documentos que no están destinados, en principio, a ser utilizados en la web, pero están incluidos en sitios web, pudiendo estar realizados, entre otros, en formato estándar Portable Document Format (PDF), o habiendo sido confeccionados mediante procesadores de texto, hojas de cálculo o aplicaciones para la realización de presentaciones.

d) Bienes de colecciones de patrimonio: Son los bienes de propiedad pública o privada que presentan un interés histórico, arqueológico, estético, científico o técnico y que forman parte de colecciones conservadas por instituciones culturales como bibliotecas, archivos y museos.

e) Contenido de los sitios web y de las aplicaciones para dispositivos móviles: Es la información tanto textual como no textual, los documentos y formularios que se pueden descargar, así como las formas de interacción bidireccional, como el tratamiento de formularios digitales y la cumplimentación de los procesos de identificación, autenticación, firma y pago.

f) Contenido multimedia de base temporal: Son los ficheros multimedia que pueden ser de los siguientes tipos: Solo audio, solo vídeo, audio y vídeo, o cualquiera de los anteriores combinado con interacción.

g) Contenidos multimedia pregrabados: Son los contenidos multimedia de base temporal emitidos en directo que se mantienen en línea o se vuelven a emitir tras su transmisión en directo, inmediatamente después de la fecha de la emisión inicial o la nueva emisión.

h) Datos de las mediciones: Son los resultados cuantificados de la actividad de seguimiento llevada a cabo a fin de comprobar la conformidad de los sitios web y las aplicaciones para dispositivos móviles con los requisitos de accesibilidad exigidos. Incluyen tanto la información cuantitativa sobre las muestras de sitios web y aplicaciones para dispositivos móviles comprobadas como la información cuantitativa sobre el nivel de accesibilidad.

i) Norma: Son las especificaciones técnicas adoptadas por un organismo de normalización reconocido, de aplicación repetida o continua, cuya observancia no es obligatoria.

j) Norma europea: Es una norma adoptada por una organización europea de normalización.

k) Norma armonizada: Es una norma europea adoptada a raíz de una petición de la Comisión Europea para la aplicación de la legislación de armonización de la Unión Europea.

l) Perceptibilidad: Es el principio de la accesibilidad que exige que la información y los componentes de la interfaz de usuario se presenten a las personas usuarias de manera que pueda percibirlos.

m) Operabilidad: Es el principio de la accesibilidad que exige que los componentes y la navegación de la interfaz de usuario se puedan utilizar por cualquier persona usuaria.

n) Comprensibilidad: Es el principio de la accesibilidad que exige que la información y el funcionamiento de la interfaz de usuario sean comprensibles por cualquier persona usuaria.

ñ) Robustez: Es el principio de la accesibilidad que exige que los contenidos sean suficientemente sólidos para poder ser interpretados de forma fiable por una gran variedad de agentes de usuario, incluidas las tecnologías de asistencia.

**Artículo 5.** *Requisitos para la accesibilidad de los sitios web y aplicaciones para dispositivos móviles.*

1. Los sitios web y aplicaciones para dispositivos móviles de las entidades obligadas incluidas en el ámbito de aplicación del presente real decreto deberán ser accesibles para sus personas usuarias y, en particular, para las personas mayores y personas con discapacidad, de modo que sus contenidos sean perceptibles, operables, comprensibles y robustos teniendo en cuenta las normas del artículo 6.

2. La accesibilidad se tendrá presente de forma integral en el proceso de diseño, gestión, mantenimiento y actualización de contenidos de los sitios web y las aplicaciones para dispositivos móviles.

3. Las entidades obligadas adoptarán, siempre que sea posible, medidas para aumentar la accesibilidad de sus sitios web y aplicaciones para dispositivos móviles respecto del nivel mínimo de accesibilidad que deba cumplirse en cada momento.

**Artículo 6.** *Presunción de conformidad con los requisitos de accesibilidad.*

1. Se presumirá que el contenido de los sitios web y aplicaciones para dispositivos móviles que cumpla las normas armonizadas o partes de éstas cuyas referencias hayan sido publicadas en el «Diario Oficial de la Unión Europea» es conforme a los requisitos de

accesibilidad establecidos en el artículo 5 que estén cubiertos por dichas normas o partes de ellas.

2. En caso de que no se hayan publicado las referencias de las normas armonizadas a que se refiere el apartado 1, se presumirá que el contenido de las aplicaciones para dispositivos móviles que cumpla las especificaciones técnicas o partes de éstas, que la Comisión haya adoptado mediante los correspondientes actos de ejecución, es conforme a los requisitos de accesibilidad establecidos en el artículo 5 que estén cubiertos por dichas especificaciones técnicas o partes de ellas.

3. En caso de que no se hayan publicado las referencias de las normas armonizadas a que se refiere el apartado 1, se presumirá que el contenido de los sitios web que cumpla los requisitos pertinentes de la norma EN 301 549 V1.1.2 (2015-04) o partes de estos, es conforme a los requisitos de accesibilidad establecidos en el artículo 5 que estén cubiertos por dichos requisitos o partes de ellos.

En caso de que no se hayan publicado las referencias de las normas armonizadas a que se refiere el apartado 1, y en ausencia de las especificaciones técnicas a que se refiere el apartado 2, se presumirá que el contenido de aplicaciones para dispositivos móviles que cumpla los requisitos pertinentes de la norma EN 301 549 V1.1.2 (2015-04) o partes de estos, es conforme a los requisitos de accesibilidad establecidos en el artículo 5 que estén cubiertos por dichos requisitos o partes de ellos.

4. Se aplicarán directamente las actualizaciones de referencias a la norma EN 301 549 V1.1.2 (2015-04) que la Comisión adopte mediante actos delegados para hacer referencia a una versión más reciente de dicha norma o a una norma europea que la sustituya.

5. El órgano encargado de realizar el seguimiento y presentación de informes ante la Comisión Europea mantendrá disponible en su sitio web la referencia concreta a las normas armonizadas, normas y especificaciones técnicas que sean de aplicación en cada momento.

**Artículo 7.** *Carga desproporcionada.*

1. Con carácter excepcional, en atención a la carga desproporcionada que el cumplimiento de los requisitos de accesibilidad pueda suponer para la entidad obligada, se podrá exceptuar el cumplimiento de los requisitos de accesibilidad recogidos en el presente real decreto.

La excepción al cumplimiento de los requisitos de accesibilidad deberá ser motivada y se limitará al contenido concreto y a lo estrictamente necesario para reducir la carga. No obstante, la entidad deberá hacer estos contenidos lo más accesibles posible y cumplir todos los requisitos de accesibilidad en el resto de contenidos.

2. Se considera carga desproporcionada aquella que impone a la entidad obligada una carga financiera y organizativa excesiva, o que compromete su capacidad para cumplir su cometido o para publicar la información necesaria y pertinente para sus tareas y servicios, teniendo en cuenta al mismo tiempo el posible beneficio o perjuicio para los ciudadanos, en particular para las personas con discapacidad y personas mayores.

3. No se consideran motivos que permitan apreciar la excepción de la carga desproporcionada la falta de prioridad, de tiempo o de conocimientos. Asimismo, tampoco es posible justificar la necesidad de adquirir o desarrollar sistemas informáticos, para la gestión de contenidos de sitios web, y aplicaciones para dispositivos móviles que no sean accesibles.

4. A fin de evaluar en qué medida el cumplimiento de los requisitos de accesibilidad previstos en este real decreto impone una carga desproporcionada, las entidades obligadas deberán tener en cuenta como mínimo las siguientes circunstancias:

a) El tamaño, los recursos y la naturaleza del sujeto concreto obligado.

b) Los costes y beneficios estimados para el mismo, en relación con los beneficios estimados para las personas con discapacidad y las personas mayores, teniendo en cuenta la frecuencia y la duración del uso del sitio web o aplicación para dispositivos móviles en especial.

5. La entidad obligada concreta que desee acogerse a la excepción contemplada en el apartado 1 de este artículo deberá llevar a cabo una evaluación inicial de la medida en que el cumplimiento de los requisitos de accesibilidad previstos en este real decreto impone una

carga desproporcionada debiéndolo hacer constar por escrito mediante el correspondiente informe. Dicha evaluación deberá revisarse al menos una vez al año para contemplar los posibles cambios organizacionales o técnicos.

6. En todo caso, en la declaración de accesibilidad para el sitio web concreto o la aplicación para dispositivos móviles concreta, después de realizar la correspondiente evaluación, se hará constar las partes de los requisitos de accesibilidad que no puede cumplir y, en su caso, se ofrecerá alternativas accesibles según los términos definidos en el artículo 15.

**Artículo 8.** *Promoción, concienciación y formación.*

1. Los organismos del sector público y otros obligados incluidos en el ámbito de aplicación del artículo 2 adoptarán medidas de sensibilización y divulgación para incrementar la concienciación dentro de las Administraciones Públicas y en la sociedad en general sobre los requisitos de accesibilidad y la universalidad de sus beneficios, así como sobre todas las medidas puestas en práctica con este real decreto, especialmente la posibilidad y medios para reclamar en caso de incumplimiento de las previsiones establecidas.

2. En particular, las entidades obligadas velarán por la concienciación en materia de accesibilidad de todo el personal a su servicio y específicamente de aquellos órganos o Unidades con competencias en el desarrollo de los sitios web y las aplicaciones para dispositivos móviles del sector público, así como de los encargados de la edición y generación de sus contenidos.

3. Las entidades obligadas fomentarán y facilitarán programas de formación internos que garanticen conocimientos actualizados sobre las condiciones de accesibilidad en la creación, gestión y actualización de los contenidos de los sitios web y aplicaciones para dispositivos móviles. Para ello:

a) Los correspondientes institutos y organismos competentes en materia de formación en la Función Pública incluirán en sus planes de formación actividades en relación con la accesibilidad de los sitios web y sus contenidos y de las aplicaciones para dispositivos móviles.

b) Las entidades obligadas establecerán, como complemento de los anteriores, programas de formación específicos en la materia para el personal a su servicio, especialmente, para quienes pertenezcan a órganos o unidades con competencias en el desarrollo de los sitios web y las aplicaciones para dispositivos móviles así como, para las personas encargadas de la edición y generación de contenidos.

4. Los organismos del sector público y otros obligados incluidos en el ámbito de aplicación del artículo 2 promoverán medidas de sensibilización, divulgación, educación y formación en el terreno de la accesibilidad, con objeto de lograr que los titulares de otros sitios web o aplicaciones móviles distintas de aquéllas a las que se refiere este real decreto, incorporen progresivamente y en la medida de lo posible los criterios de accesibilidad, particularmente aquéllas cuyo contenido se refiera a bienes y servicios a disposición del público.

5. Respecto de las webs y dispositivos móviles, los organismos del sector público y otros obligados incluidos en el ámbito de aplicación del artículo 2 observarán los mandatos sobre promoción de la accesibilidad universal contenidos en las disposiciones normativas específicas en materia de contratación pública y harán uso de las facultades y posibilidades que esta legislación ofrece a los órganos contratantes, para ampliar y elevar los niveles de accesibilidad digital en la adquisición de bienes, productos y servicios.

**Artículo 9.** *Participación de las personas interesadas.*

Las Administraciones Públicas determinarán los mecanismos de participación de las personas interesadas y de las personas usuarias en el seguimiento de las políticas de accesibilidad de los sitios web y las aplicaciones para dispositivos móviles, teniendo en cuenta especialmente a las organizaciones representativas de personas con discapacidad y personas mayores, y sus familias.

CAPÍTULO II

**Comunicaciones, quejas y reclamaciones**

**Artículo 10.** *Mecanismos de comunicación.*

1. Las entidades obligadas deberán ofrecer a las personas usuarias un mecanismo de comunicación que permita a cualquier persona presentar sugerencias y quejas, así como informar sobre cualquier posible incumplimiento por parte de su sitio web o de su aplicación para dispositivos móviles de los requisitos de accesibilidad y solicitar la información excluida.

2. Se distinguen dos modalidades en función de la naturaleza de la comunicación y de los efectos y tratamiento que ésta vaya a tener:

a) Comunicaciones sobre requisitos de accesibilidad. Permite a cualquier persona física y jurídica informar sobre cualquier posible incumplimiento por parte del sitio web o de la aplicación para dispositivos móviles de los requisitos de accesibilidad establecidos. También permite transmitir otras dificultades de acceso al contenido o formular cualquier otra consulta o sugerencia de mejora relativa a la accesibilidad del sitio web o aplicación para dispositivos móviles.

b) Solicitudes de información accesible y quejas. Permite a cualquier persona física o jurídica formular quejas relativas al cumplimiento de los requisitos de este real decreto y solicitar la información relativa a contenidos que están excluidos del ámbito de aplicación de este real decreto según lo establecido por el artículo 3, apartado 4, o exentos del cumplimiento de los requisitos de accesibilidad por imponer una carga desproporcionada.

**Artículo 11.** *Comunicaciones sobre requisitos de accesibilidad.*

Las comunicaciones sobre requisitos de accesibilidad podrán presentarse mediante medios electrónicos habilitando una dirección de correo electrónico específica o un formulario que permita la presentación telemática. Adicionalmente, se habilitará al menos uno de los siguientes canales complementarios al electrónico: Un teléfono o una oficina física de atención.

**Artículo 12.** *Solicitudes de información accesible y quejas.*

1. Las solicitudes de información accesible y quejas serán presentadas y registradas conforme a los requisitos establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

2. En el caso de las solicitudes de información accesible, la persona interesada deberá concretar, con toda claridad, los hechos, razones y petición que permitan constatar que se trata de una solicitud razonable y legítima.

3. Recibidas las solicitudes de información accesible y quejas, la entidad obligada deberá responder a la persona interesada en el plazo de veinte días hábiles.

4. El transcurso de dicho plazo se podrá suspender en el caso de que deba requerirse a la persona interesada para que, en un plazo de diez días hábiles, formule las aclaraciones necesarias para la correcta tramitación de la solicitud de información accesible o queja. Transcurrido dicho plazo sin que la persona interesada haya realizado las aclaraciones oportunas, se continuará con su tramitación.

5. La respuesta deberá incluir la siguiente información:

a) La Unidad que emite la respuesta.

b) La decisión que se ha adoptado.

c) En su caso, la información accesible solicitada.

d) En su caso, el plazo estimativo y la Unidad responsable de llevar a cabo las medidas para corregir un posible incumplimiento, si las mismas no se pueden adoptar de inmediato.

e) La Unidad ante la cual se puede reclamar y el procedimiento por el cual se puede hacer la reclamación.

6. Transcurrido el plazo máximo para resolver sin que se haya notificado la respuesta se entenderá que la solicitud de información accesible no ha sido aceptada o que la queja no ha sido considerada.

Téngase en cuenta que se declara que los apartados 1, 3, 4 y 6 invaden las competencias autonómicas y carecen de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

**Artículo 13.** *Procedimiento de reclamación.*

1. Si una vez realizada una solicitud de información accesible o queja, ésta hubiera sido desestimada, no se estuviera de acuerdo con la decisión adoptada, o la respuesta no cumpliera los requisitos contemplados en el artículo 12.5, la persona interesada podrá iniciar una reclamación para conocer y oponerse a los motivos de la desestimación, instar la adopción de las medidas oportunas en el caso de no estar de acuerdo con la decisión adoptada, o exponer las razones por las que se considera que la respuesta no cumple con los requisitos exigidos.

Igualmente se podrá iniciar una reclamación en el caso de que haya trascurrido el plazo **de veinte días hábiles** sin haber obtenido respuesta.

2. Dicha reclamación deberá ser presentada y registrada conforme a los requisitos establecidos en la Ley 39/2015, de 1 de octubre.

La reclamación deberá dirigirse a la Unidad responsable de accesibilidad de ese ámbito competencial, o si la respuesta se hubiera realizado desde la propia Unidad responsable de accesibilidad, al superior jerárquico de ésta.

3. Las entidades obligadas deberán incluir en la declaración de accesibilidad la Unidad a la cual elevar las reclamaciones junto con el enlace al sistema de registro en el que se deberá realizar dicha reclamación.

4. Recibida la reclamación, la Unidad responsable de atenderla deberá responder a la persona interesada en el plazo máximo de dos meses.

5. El transcurso de dicho plazo se podrá suspender en el caso de que deba requerirse a la persona interesada para que, en un plazo de diez días hábiles, formule las aclaraciones necesarias para la correcta tramitación de la reclamación. Transcurrido dicho plazo sin que la persona interesada haya realizado las aclaraciones oportunas, se continuará con la tramitación de la reclamación.

6. Transcurrido el plazo máximo para resolver la reclamación sin que se haya notificado la resolución de la misma, se entenderá que la reclamación ha sido desestimada.

Téngase en cuenta que se declara que el inciso destacado del apartado 1 y los apartados 2 a 6 invaden las competencias autonómicas y carecen de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

**Artículo 14.** *Recursos.*

Contra la resolución de la reclamación regulada en los anteriores artículos se podrán interponer los recursos administrativos que procedan, de conformidad con lo dispuesto en el artículo 112 de la Ley 39/2015, de 1 de octubre de 2015.

## CAPÍTULO III

## Control, revisión, seguimiento y presentación de informes

**Artículo 15.** *Declaración de accesibilidad.*

1. Las entidades responsables de las webs y aplicaciones para móviles proporcionarán una declaración de accesibilidad detallada, exhaustiva y clara sobre la conformidad de sus respectivos sitios web y aplicaciones para dispositivos móviles con lo dispuesto en este real

decreto. Dicha declaración será actualizada periódicamente, como mínimo una vez al año, o cada vez que se realice una revisión de accesibilidad conforme a lo especificado en el artículo 17.

Esta declaración de accesibilidad se proporcionará en un formato accesible haciendo uso de las instrucciones y del modelo de declaración de accesibilidad que se establezca conforme a lo dispuesto en el apartado 3.

En el caso de los sitios web, la declaración se publicará en el sitio web correspondiente estando disponible su acceso desde todas las páginas del sitio web con un enlace denominado «Accesibilidad» o su equivalente en el idioma en el que se encuentre disponible la página.

En el caso de las aplicaciones para dispositivos móviles, la declaración estará disponible en el sitio web de la entidad obligada que haya desarrollado la aplicación concreta para dispositivos móviles junto con el enlace para su descarga o bien se facilitará junto con otra información disponible al descargar la aplicación de las plataformas de distribución de aplicaciones.

2. La declaración de accesibilidad comprenderá, como mínimo, la siguiente información:

a) Una explicación sobre aquellas partes del contenido que no sean accesibles y las razones de dicha inaccesibilidad, así como, en su caso, las alternativas accesibles que se ofrezcan.

b) Un enlace y descripción del mecanismo de comunicación en los términos que se establecen en los artículos 10, 11 y 12 del presente real decreto.

c) Un enlace al procedimiento de reclamación regulado en el artículo 13 al que cualquier persona interesada pueda recurrir en caso de que la respuesta a la comunicación o a la solicitud sea insatisfactoria.

3. Mediante Orden de la Ministra de Política Territorial y Función Pública se aprobarán instrucciones específicas para la generación y puesta a disposición de las declaraciones de accesibilidad **de aplicación en todo el territorio nacional** de acuerdo con los requisitos especificados en el modelo europeo.

> Téngase en cuenta que se declara inconstitucional y nulo el inciso destacado del apartado 3 y que el texto restante de dicho apartado invade las competencias autonómicas y carece de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

**Artículo 16.** *Unidad responsable de accesibilidad.*

1. Cada entidad obligada determinará la Unidad responsable de garantizar el cumplimiento de los requisitos de accesibilidad de los sitios web y aplicaciones para dispositivos móviles dentro de su ámbito competencial.

En la Administración General del Estado se designarán las Unidades responsables de accesibilidad en el ámbito de las Subsecretarías de cada Departamento considerando todos los posibles organismos públicos y entidades de derecho público dependientes de ese Departamento.

En las comunidades autónomas se designará la Unidad responsable de accesibilidad para todo el ámbito autonómico.

En las entidades locales y demás organismos obligados se designará, conforme a sus características organizativas propias, la Unidad responsable de accesibilidad de su ámbito.

2. La Unidad responsable de accesibilidad definirá el modelo de funcionamiento dentro de su ámbito competencial actuando directamente sobre todo el ámbito o con un posible esquema de responsables de accesibilidad delegados en los diferentes organismos o entidades dependientes.

Téngase en cuenta que se declara que el apartado 2 invade las competencias autonómicas y carece de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

3. La Unidad responsable de accesibilidad tendrá las siguientes funciones:

a) Coordinar y velar por el funcionamiento efectivo de los mecanismos de comunicación establecidos en el capítulo II ayudando a la definición, emitiendo directrices y promoviendo la existencia de los medios y procedimientos para garantizar una adecuada gestión y atención de cuantas consultas, sugerencias, comunicaciones, quejas y solicitudes de información accesible se reciban en cada uno de los órganos, organismos o entidades bajo su competencia.

b) Atender y dar respuesta a las reclamaciones que, en aplicación de lo dispuesto en el artículo 13 le sean dirigidas.

c) Revisar las evaluaciones realizadas para acogerse a la excepción del cumplimiento de los requisitos de accesibilidad por imponer éstos una carga desproporcionada regulada en el artículo 7.

d) Coordinar las revisiones periódicas de accesibilidad establecidas en el artículo 17, con la colaboración, en su caso, de las Unidades de tecnologías de la información y comunicaciones.

e) Coordinar y fomentar las actividades de promoción, concienciación y formación establecidas en el artículo 8.

f) Realizar los informes que se determinen para garantizar el cumplimiento de las previsiones establecidas en el artículo 19.

g) Actuar como punto de contacto con el organismo encargado de realizar el seguimiento y presentación de informes y colaborar con las tareas que tiene asignadas

h) Cualesquiera otras, que en garantía de la accesibilidad de los sitios web y aplicaciones para dispositivos móviles le puedan ser atribuidas.

4. Se deberá notificar al órgano encargado de realizar el seguimiento y presentación de informes al que se refiere el artículo 18 las designaciones, modificaciones o bajas de las correspondientes Unidades responsables de accesibilidad.

**Artículo 17.** *Revisión de la accesibilidad.*

1. Las entidades obligadas por el presente real decreto realizarán revisiones del cumplimiento de los requisitos de accesibilidad establecidos tanto en la fase de diseño de los sitios web y aplicaciones para dispositivos móviles como antes de su puesta en funcionamiento.

2. Una vez puesto en funcionamiento un sitio web o aplicación para dispositivos móviles, las entidades obligadas realizarán revisiones periódicas del cumplimiento de los requisitos de accesibilidad con el fin de garantizar el mantenimiento de su cumplimiento a lo largo del tiempo. Especialmente, se deberá tener en cuenta el caso de los contenidos añadidos o modificados durante el ciclo de vida de los sitios web así como las actualizaciones tecnológicas de estos últimos y de las aplicaciones para dispositivos móviles.

3. Las revisiones de accesibilidad deberán abarcar todos los requisitos exigidos y tendrán en consideración tanto aspectos de revisión automática como aspectos de revisión manual experta. El resultado de éstas deberá quedar recogido en un informe de revisión de la accesibilidad.

4. Mediante Orden de la Ministra de Política Territorial y Función Pública se podrá aprobar un modelo y condiciones específicas para realizar estas revisiones de accesibilidad que podrán ampliar lo establecido en la metodología europea para el seguimiento de la conformidad. En cualquier caso, estas revisiones deberán respetar las condiciones mínimas exigidas para las revisiones en profundidad de un sitio web o aplicación móvil que establezca la metodología europea.

Téngase en cuenta que se declara que la primera frase del apartado 4 invade las competencias autonómicas y carece de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

5. Las entidades obligadas podrán certificar el cumplimiento de los requisitos de este real decreto en sus sitios web y aplicaciones para dispositivos móviles por una entidad de certificación cuya competencia técnica haya sido reconocida formalmente por la Entidad Nacional de Acreditación (ENAC) o por otro organismo nacional de acuerdo al Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93.

6. En cualquier caso, la primera revisión de accesibilidad deberá haberse realizado en el caso de los sitios web antes de dos años desde la entrada en vigor de este real decreto, y, en el caso de las aplicaciones móviles, antes de tres años desde la entrada en vigor de este real decreto.

**Artículo 18.** *Seguimiento y presentación de informes.*

1. El órgano encargado de realizar el seguimiento y presentación de informes ante la Comisión Europea es el Ministerio de Política Territorial y Función Pública.

2. Este órgano podrá comprobar periódicamente el estado de situación con respecto a la conformidad de los sitios web y las aplicaciones para dispositivos móviles de los organismos del sector público con los requisitos de accesibilidad, basándose en la metodología para el seguimiento de la conformidad prevista en el artículo 8.2 de la Directiva (UE) 2016/2102, del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público según sea determinado por la Comisión Europea en los correspondientes actos de ejecución.

Este órgano también podrá realizar verificaciones sobre muestras aleatorias con respecto a la exactitud de los informes de revisión de la accesibilidad definidos en el artículo 17.

3. Este órgano presentará a la Comisión Europea, a más tardar el 23 de diciembre de 2021 y posteriormente cada tres años, un informe sobre el resultado del seguimiento que se hará público en formato accesible.

4. Dicho informe deberá ajustarse a lo que se determine en los actos de ejecución que adoptará la Comisión Europea para la presentación de informes de Directiva (UE) 2016/2102, del Parlamento Europeo y del Consejo, de 26 de octubre de 2016. En cualquier caso deberá incluir:

a) Los datos de las mediciones.

b) Información sobre el uso del procedimiento de reclamación establecido en el artículo 13.

c) Información sobre los elementos enumerados en el apartado 5 cuando hayan sido objeto de cambios significativos respecto del informe anterior.

5. El primer informe comprenderá también:

a) Una descripción de los mecanismos creados en España para consultar a las personas interesadas sobre la accesibilidad de los sitios web y las aplicaciones para dispositivos móviles;

b) procedimientos para hacer pública cualquier evolución de las políticas de accesibilidad relacionada con los sitios web y las aplicaciones para dispositivos móviles;

c) experiencias y conclusiones extraídas de la aplicación de las normas sobre conformidad con los requisitos de accesibilidad establecidos;

d) información sobre actividades de formación y concienciación.

**Artículo 19.** *Coordinación para el seguimiento y presentación de informes.*

1. Cada Unidad responsable de accesibilidad preparará tres informes anuales sobre su ámbito de actuación concreto que tendrá disponibles antes del 1 de octubre de cada año a partir del año 2020:

a) Informe sobre la atención de quejas y reclamaciones. Dicho informe incluirá las medidas puestas en práctica para atender las cuestiones planteadas en el artículo 16.3.a) junto a un estudio de las comunicaciones, consultas, sugerencias, solicitudes de información accesible y quejas formuladas a través del mismo. También incluirá un estudio de las reclamaciones atendidas y revisiones realizadas según el artículo 16.3.b) y c).

b) Informe de seguimiento sobre el cumplimiento de los requisitos de accesibilidad dentro de su ámbito competencial incluyendo las medidas puestas en marcha para atender las acciones contempladas en el artículo 16.3.d) y los resultados derivados de ellas. Asimismo, se incluirán todos los informes de revisión de la accesibilidad realizados según lo previsto en el artículo 17.

c) Informe de seguimiento sobre la promoción, concienciación y formación dentro de su ámbito competencial incluyendo las medidas puestas en marcha para atender las acciones contempladas en el artículo 16.3.e) y los resultados derivados de ellas.

2. Para facilitar las tareas del Ministerio de Política Territorial y Función Pública colaborarán con éste: La Red de Contactos de Accesibilidad Digital de las Administraciones Públicas del artículo 20, todas las Unidades responsables de accesibilidad y todos los actores implicados en las diferentes actividades de revisión de la accesibilidad, procedimiento de reclamación, promoción y concienciación, formación, y coordinación previstas en el presente real decreto.

Para ello deberán suministrar la información específica en tales áreas con los modelos, condicionantes y procedimientos que establezca el Ministerio de Política Territorial y Función Pública.

3. **Para la definición de los modelos, condicionantes y procedimientos que permitan conocer regularmente e informar** sobre estas materias, **el Ministerio de Política Territorial y Función Pública** podrá contar con la participación de:

a) La Red de Contactos de Accesibilidad Digital de las Administraciones Públicas.

b) Los órganos de coordinación en materia de tecnologías de la información de la Administración General del Estado previstos en el Real Decreto 806/2014, de 19 de septiembre.

c) La Comisión Sectorial de Administración Electrónica establecida en la disposición adicional novena de la Ley 40/2015, de 2 de octubre, de Régimen Jurídico del Sector Público.

d) El Comité Técnico Estatal De La Administración Judicial Electrónica establecido en el artículo 44 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

> Téngase en cuenta que se declara que el inciso destacado del apartado 3 invade las competencias autonómicas y carecen de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

**Artículo 20.** *Red de Contactos de Accesibilidad Digital de las Administraciones Públicas.*

1. Se crea la Red de Contactos de Accesibilidad Digital de las Administraciones Públicas con funciones de asistencia al Ministerio de Política Territorial y Función Pública regulado en el artículo 18, que tendrá la consideración de grupo de trabajo de los previstos en el artículo 22.3 de la Ley 40/2015, de 1 de octubre.

2. La Red de Contactos de Accesibilidad Digital de las Administraciones Públicas estará integrada por:

a) Las personas titulares de las Unidades responsables de accesibilidad de la Administración General del Estado.

b) Las personas titulares de las Unidades responsables de accesibilidad de las comunidades autónomas.

c) Al menos un punto de contacto provincial que agrupará a las entidades locales de esa provincia y que podrá estar provisto por la correspondiente Diputación Provincial, Comunidad Autónoma, Consorcio o Federación de municipios considerando sus características territoriales concretas y de acuerdo con la normativa específica de régimen local.

d) Una persona designada al respecto por parte de la Conferencia de Rectores para las Universidades españolas que agrupará a las Universidades.

e) Una persona designada al respecto por parte del Comité Técnico Estatal de la Administración Judicial Electrónica que agrupará a las entidades del ámbito judicial.

f) Las personas titulares de las Unidades responsables de accesibilidad de los demás entes obligados que no estén cubiertos por los anteriormente indicados.

g) Las asociaciones comprendidas en el artículo 2.1.e participarán a través de uno de los miembros anteriormente indicados considerando el tipo de la entidad con participación mayoritaria en la asociación.

3. Los personas integrantes de esta red de contactos actuarán como difusoras y agregadoras de la información disponible de todas las entidades a las que representen o agrupen.

4. Las designaciones, modificaciones o bajas de las personas integrantes de esta red deberán ser notificadas al Ministerio de Política Territorial y Función Pública.

**Disposición adicional primera.** *Criterios de accesibilidad aplicables a los sitios web y aplicaciones para dispositivos móviles con financiación pública.*

Las Administraciones Públicas exigirán que se apliquen los criterios de accesibilidad de los artículos 5 y 6 del presente real decreto a:

a) Los sitios web y aplicaciones para dispositivos móviles que reciban financiación pública para su diseño o mantenimiento.

b) Los sitios web y aplicaciones para dispositivos móviles, vinculados a la prestación de servicios públicos, de entidades y empresas que se encarguen, ya sea por vía concesional o a través de otra vía contractual, de gestionar servicios públicos, en especial, los que tengan carácter educativo, sanitario, cultural, deportivo y de servicios sociales.

c) Los sitios web y aplicaciones para dispositivos móviles de los centros privados educativos, de formación y universitarios sostenidos, total o parcialmente, con fondos públicos.

**Disposición adicional segunda.** *Criterios de accesibilidad aplicables a los sitios web y aplicaciones para dispositivos móviles de los órganos constitucionales del Estado y de los órganos legislativos y de control autonómicos.*

Los criterios de accesibilidad recogidos en el presente real decreto, serán de aplicación a los sitios web y aplicaciones para dispositivos móviles de los órganos competentes del Congreso de los Diputados, del Senado, del Consejo de Estado, del Consejo Económico y Social, del Consejo General del Poder Judicial, del Tribunal Constitucional, del Tribunal de Cuentas, del Defensor del Pueblo, del Banco de España, **de las Asambleas legislativas de las comunidades autónomas**, así como a las instituciones autonómicas que realicen funciones análogas, en relación con sus actividades sujetas a Derecho Administrativo y con sujeción a su normativa específica.

Téngase en cuenta que se declara inconstitucional y nulo el inciso destacado, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

El titular de la Unidad responsable de accesibilidad de cada uno de estos órganos podrá formar parte, si así lo decide la institución concernida, de la Red de Contactos de Accesibilidad Digital de las Administraciones Públicas.

**Disposición adicional tercera.** *Lenguas de signos españolas y medios de apoyo a la comunicación oral.*

Respecto de las lenguas de signos españolas y los medios de apoyo a la comunicación oral, los sitios web y las aplicaciones móviles tendrán en cuenta lo que disponga específicamente la Ley 27/2007, de 23 de octubre, por la que se reconocen las lenguas de signos españolas y se regulan los medios de apoyo a la comunicación oral de las personas sordas, con discapacidad auditiva y sordociegas y sus normas de desarrollo.

**Disposición adicional cuarta.** *No incremento de gastos de personal y Unidades responsables de accesibilidad en la Administración General del Estado.*

Conforme a lo establecido en la disposición adicional trigésima novena de la Ley 6/2018, de 3 de julio, de Presupuestos Generales del Estado para el año 2018, las medidas incluidas en esta norma no podrán suponer en el ámbito de la Administración General del Estado incremento de dotaciones, ni de retribuciones, ni de otros gastos de personal.

Las funciones que corresponda desarrollar a las Unidades responsables de accesibilidad serán asignadas a Unidades ya existentes.

**Disposición transitoria única.** *Modelo de declaración.*

En tanto no se publique el modelo de declaración al que se refiere el artículo 15, se aplicará por defecto el modelo de declaración de accesibilidad que la Comisión Europea establezca mediante los correspondientes actos de ejecución previstos en la Directiva (UE) 2016/2102, de 26 de octubre de 2016.

> Téngase en cuenta que se declara que esta disposición invade las competencias autonómicas y carece de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

**Disposición derogatoria única.**

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en el presente real decreto y, específicamente, los artículos 5, 6 y 7 del Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.

**Disposición final primera.** *Modificación del Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social, aprobado por el Real Decreto 1494/2007, de 12 de noviembre.*

El artículo 9 del Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social, aprobado por el Real Decreto 1494/2007, de 12 de noviembre, quedará redactado en la forma siguiente:

> **«Artículo 9.** *Condiciones básicas de accesibilidad en servicios y productos de confianza.*
>
> Los servicios de confianza prestados y los productos para las personas usuarias finales utilizados en la prestación de estos servicios deberán ser accesibles para las

personas mayores y personas con discapacidad. Excepcionalmente, esta obligación no será aplicable cuando el producto o servicio de confianza no disponga de una solución tecnológica que permita su accesibilidad.»

**Disposición final segunda.** *Título competencial.*

La presente norma se dicta al amparo de lo dispuesto en el artículo 149.1.1.ª y 18.ª de la Constitución, que atribuye al Estado las competencias para «la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales» y, para regular «las bases del régimen jurídico de las Administraciones Públicas y el procedimiento administrativo común», respectivamente.

**Disposición final tercera.** *Incorporación de derecho comunitario.*

Mediante el presente real decreto se incorpora al ordenamiento jurídico la Directiva (UE) 2016/2102, del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.

**Disposición final cuarta.** *Desarrollo normativo.*

Se faculta a los titulares del Ministerio de Política Territorial y Función Pública y del Ministerio de Economía y Empresa, en el ámbito de sus respectivas competencias, para dictar las disposiciones adicionales necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, así como para acordar las medidas precisas para garantizar su ejecución e implantación efectiva, sin perjuicio de las competencias propias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

**Disposición final quinta.** *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado» con las siguientes excepciones:

Para los sitios web, las disposiciones previstas en los artículos 10.2.b), 12 y 13 serán de aplicación al año de la entrada en vigor de este real decreto, y a los dos años para los sitios web ya publicados.

Todas las disposiciones relativas a aplicaciones para dispositivos móviles serán de aplicación desde el 23 de junio de 2021.

# § 11

## Resolución de 21 de marzo de 2013, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Guía de Comunicación Digital para la Administración General del Estado

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 79, de 2 de abril de 2013
Última modificación: sin modificaciones
Referencia: BOE-A-2013-3528

En los últimos años, la comunicación con los ciudadanos y las empresas por medios digitales a través de portales web, sedes electrónicas, blogs, o redes sociales, a los que en adelante en esta resolución se denominarán bajo el término genérico de sitios web, ha adquirido una importancia indiscutible para la Administración General del Estado (AGE) conformándose como una herramienta indispensable para la difusión de sus contenidos y para fortalecer la participación ciudadana e impulsar la transparencia de la actividad pública.

Además, cabe recordar que como consecuencia de la aplicación de la Ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos y del Título II del Real Decreto 1671/2009, de 6 de noviembre, de desarrollo parcial de dicha Ley, la AGE ofrece actualmente la tramitación electrónica de la práctica totalidad de los servicios administrativos en sus sedes electrónicas.

Los estudios sobre el uso en un futuro próximo de los sitios web de las administraciones públicas coinciden en señalar que su utilización se va a incrementar, en primer lugar, por el perfil de los usuarios, los llamados nativos digitales, cuyo modo de relación natural con las administraciones será a través de los medios digitales y en segundo lugar, por la generalización en el uso de dispositivos móviles de tercera y cuarta generación que permitirán acceder e interactuar con dichos medios digitales con una mayor facilidad.

En este contexto, es esencial reforzar la confianza de los usuarios en los sitios web de la AGE ya sea como medio de información, de participación o para la utilización de los servicios de las sedes electrónicas y es necesario también mejorar la usabilidad y la calidad de dichos sitios web, mediante el impulso de la normalización de características tales como su apariencia y sus condiciones de uso, así como mediante el cumplimiento de los requisitos normativos.

Así, la «Guía de Comunicación Digital para la Administración General del Estado» presenta un marco de criterios, recomendaciones y buenas prácticas a tener en cuenta por los Departamentos y Organismos vinculados o dependientes de la AGE, tanto al crear nuevos sitios web como al dotarlos de contenidos o evolucionar y mantener los sitios ya existentes.

La Guía también recopila la abundante normativa aplicable a los sitios web de la AGE y en particular, en materia de: imagen institucional, multilingüismo, accesibilidad o seguridad.

La presente Guía actualiza: la «Guía para la edición y publicación de las páginas web de la Administración General del Estado» de 2005 y de 2008; el «Borrador de la Guía de

páginas web de la AGE» de 2009 y la «Guía de Sedes electrónicas» de 2010, reuniendo dichos documentos en uno único y ampliándolos con indicaciones a la hora de dotar de contenidos a los sitios web o sobre la presencia de la AGE en las redes sociales, que no se contemplaban en los citados documentos.

La «Guía de Comunicación Digital para la Administración General del Estado» se divide en ocho fascículos, que pueden ser utilizados conjunta o independientemente y dos anexos técnicos.

Los fascículos se refieren a diversas materias como son: Aspectos Generales que trata de la navegación, la legibilidad, las consideraciones técnicas, los sitios para dispositivos móviles y el acceso con autenticación; Imagen Institucional que indica el uso de los logotipos del Gobierno de España en los sitios web, el uso de elementos distintivos de imagen en las redes sociales o la imagen promocional de la administración electrónica; Multilingüismo; Accesibilidad; Seguridad; Aspectos de Comunicación; Tecnologías web 2.0 (blogs, cuentas o perfiles de redes sociales), que contiene las recomendaciones sobre los contenidos y las normas de participación en las redes sociales y por último, Mejora y Mantenimiento en el que se aconseja sobre las técnicas y métricas a utilizar en los sitios web una vez puestos en marcha.

Los anexos técnicos se refieren a los Perfiles, que contiene una descripción de los recursos humanos necesarios para las distintas tareas a realizar en la puesta en marcha o mantenimiento de los sitios web de la AGE y a la Normativa que recopila la legislación ya publicada que es de aplicación en este ámbito.

La «Guía de Comunicación Digital para la Administración General del Estado» ha sido elaborada por el Ministerio de Hacienda y Administraciones Públicas, concretamente por la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica de la Secretaría de Estado para la Administración Pública, en colaboración con la Secretaría de Estado de Comunicación del Ministerio de la Presidencia.

La presente Guía ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica con la participación de todos los Departamentos Ministeriales a los que les es de aplicación.

Atendiendo a la complejidad y diversidad de aspectos que hay que tener en cuenta al elaborar y mantener los sitios web de la AGE, se considera necesaria la publicación de esta resolución de la Secretaría de Estado de Administraciones Públicas, la cual aprueba e insta a la aplicación de la «Guía de Comunicación Digital para la Administración General del Estado», que aglutina los criterios y recomendaciones y clarifica las instrucciones que deban ser observadas al respecto por los distintos departamentos y organismos de la AGE.

En consecuencia, en virtud de las competencias atribuidas por el artículo 16.1 e), f) y g) del Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas, resuelvo:

**Primero.** *Aprobación y aplicación de la «Guía de Comunicación Digital para la Administración General del Estado».*

1. Se aprueba la «Guía de Comunicación Digital para la Administración General del Estado», que estará disponible en el Portal de la Administración Electrónica. (http://www.administracionelectronica.gob.es)

2. Los sitios web, elaborados por los Departamentos u Organismos Públicos vinculados o dependientes de la AGE para cualquier tipo de dispositivo, procurarán observar las recomendaciones, criterios y buenas prácticas establecidos en dicha Guía, de manera gradual en la medida en que sus circunstancias, en cuanto a recursos humanos y disponibilidad presupuestaria, lo permitan.

**Segundo.** *Actualización de la Guía.*

La Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, oída la Comisión Permanente del Consejo Superior de Administración Electrónica llevará a cabo la actualización de la «Guía de Comunicación Digital para la Administración General del Estado» cuando lo considere necesario.

**Tercero.** *Difusión de la Guía.*

La presente Guía y sus futuras versiones se distribuirán a los Departamentos y Organismos a través de la Comisión Permanente del Consejo Superior de Administración Electrónica y se publicarán en el apartado de Documentación: Metodologías y Guías del Portal de la Administración Electrónica: http://www.administracionelectronica.gob.es.

Los elementos relativos a la Imagen Institucional para contribuir al cumplimiento de los criterios establecidos en esta Guía se facilitarán a los Departamentos y Organismos en el espacio: http://imagen.funciona.es/ al que se accede a través de la Red SARA.

**Cuarto.** *Aplicación.*

La «Guía de Comunicación Digital para la Administración General del Estado» que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

**Quinto.** *Pérdida de efectos.*

La presente Resolución sustituye a las siguientes disposiciones, que quedan sin efecto:

– «Resolución de 9 de marzo de 2005 de la Secretaria General para la Administración Pública por la que se aprueba la Guía para la edición y publicación de páginas web en la Administración General del Estado».

– El apartado Cuarto y el Anexo II de la "Resolución de 2 de abril de 2007, de la Secretaría General para la Administración Pública (BOE de 16 de abril), por la que se modifica el Manual de Imagen Institucional de la Administración General del Estado y la Guía para la edición y publicación de páginas web en la Administración General del Estado aprobada por Resolución de 9 de marzo de 2005 de la Secretaría General para la Administración Pública."

# § 11 Guía de Comunicación Digital para la Administración General del Estado

**Información relacionada**

- Véase la Resolución de 26 de marzo de 2024, de la Secretaría de Estado de Función Pública, por la que se actualiza el Manual de Imagen Institucional adaptándolo a la nueva estructura de vicepresidencias del Gobierno y departamentos ministeriales de la Administración General del Estado. Ref. BOE-A-2024-6708
- Véase la Resolución de 28 de noviembre de 2023, de la Secretaría de Estado de Función Pública, por la que se actualiza el Manual de Imagen Institucional adaptándolo a la nueva estructura de vicepresidencias del Gobierno y departamentos ministeriales de la Administración General del Estado. Ref. BOE-A-2023-24599
- Véase la Resolución de 15 de junio de 2022, por la que se aprueba la actualización del fascículo 2 de la «Guía de Comunicación Digital para la Administración General del Estado», que estará disponible en el Portal de Imagen Institucional https://imagen.funciona.es. Ref. BOE-A-2022-10329
- Véase la Resolución de 21 de septiembre de 2021, por la que se actualiza el Manual de Imagen Institucional, adaptándolo a la nueva estructura de departamentos ministeriales de la Administración General del Estado. Ref. BOE-A-2021-16826
- Véase la Resolución de 28 de febrero de 2020, por la que se actualiza el Manual de Imagen Institucional, adaptándolo a la nueva estructura de departamentos ministeriales de la Administración General del Estado. Ref. BOE-A-2020-3296
- Véase la Resolución de 10 de julio de 2018, por la que se actualiza el Manual de Imagen Institucional, adaptándolo a la nueva estructura de departamentos ministeriales de la Administración General del Estado. Ref. BOE-A-2018-10638
- Véase la Resolución de 3 de abril de 2017, por la que se actualiza el Manual de Imagen Institucional, adaptándolo a la nueva estructura de departamentos ministeriales de la Administración General del Estado. Ref. BOE-A-2017-4178

# § 12

## Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

Ministerio de la Presidencia
«BOE» núm. 25, de 29 de enero de 2010
Última modificación: 31 de marzo de 2021
Referencia: BOE-A-2010-1331

I

La interoperabilidad es la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos. Resulta necesaria para la cooperación, el desarrollo, la integración y la prestación de servicios conjuntos por las Administraciones públicas; para la ejecución de las diversas políticas públicas; para la realización de diferentes principios y derechos; para la transferencia de tecnología y la reutilización de aplicaciones en beneficio de una mejor eficiencia; para la cooperación entre diferentes aplicaciones que habiliten nuevos servicios; todo ello facilitando el desarrollo de la administración electrónica y de la sociedad de la información.

En el ámbito de las Administraciones públicas, la consagración del derecho de los ciudadanos a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas. Esta obligación tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, así como la remoción de los obstáculos que impidan o dificulten el ejercicio pleno del principio de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías de la información y las comunicaciones, garantizando con ello la independencia en la elección de las alternativas tecnológicas por los ciudadanos, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoce el protagonismo de la interoperabilidad y se refiere a ella como uno de los aspectos en los que es obligado que las previsiones normativas sean comunes y debe ser, por tanto, abordado por la regulación del Estado. La interoperabilidad se recoge dentro del principio de cooperación en el artículo 4 y tiene un protagonismo singular en el título cuarto dedicado a la Cooperación entre Administraciones para el impulso de la administración electrónica. En dicho título el aseguramiento de la interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones públicas figura en el artículo 40 entre las funciones del órgano de cooperación en esta materia, el Comité Sectorial de Administración Electrónica. A continuación, el artículo 41 se refiere a la aplicación por parte de las Administraciones públicas de las medidas informáticas, tecnológicas y organizativas, y de

seguridad, que garanticen un adecuado nivel de interoperabilidad técnica, semántica y organizativa y eviten discriminación a los ciudadanos por razón de su elección tecnológica. Y, seguidamente, el artículo 42.1 crea el Esquema Nacional de Interoperabilidad que comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad, entre éstas y con los ciudadanos.

La finalidad del Esquema Nacional de Interoperabilidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

II

El Esquema Nacional de Interoperabilidad tiene presentes las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones públicas, así como los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos, así como en su caso y, de forma complementaria, estándares de uso generalizado por los ciudadanos.

Su articulación se ha realizado atendiendo a la normativa nacional sobre acceso electrónico de los ciudadanos a los servicios públicos, protección de datos de carácter personal, firma electrónica y documento nacional de identidad electrónico, accesibilidad, uso de lenguas oficiales, reutilización de la información en el sector público y órganos colegiados responsables de la administración electrónica. Se han tenido en cuenta otros instrumentos, tales como el Esquema Nacional de Seguridad, desarrollado al amparo de lo dispuesto en la Ley 11/2007, de 22 de junio, o antecedentes como los Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades.

En términos de las recomendaciones de la Unión Europea se atiende al Marco Europeo de Interoperabilidad, elaborado por el programa comunitario IDABC, así como a otros instrumentos y actuaciones elaborados por este programa y que inciden en alguno de los múltiples aspectos de la interoperabilidad, tales como el Centro Europeo de Interoperabilidad Semántica, el Observatorio y Repositorio de Software de Fuentes Abiertas y la Licencia Pública de la Unión Europea. También se atiende a la Decisión 922/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa a las soluciones de interoperabilidad para las administraciones públicas europeas, a los planes de acción sobre administración electrónica en materia de interoperabilidad y de aspectos relacionados, particularmente, con la política comunitaria de compartir, reutilizar y colaborar.

III

Este real decreto se limita a establecer los criterios y recomendaciones, junto con los principios específicos necesarios, que permitan y favorezcan el desarrollo de la interoperabilidad en las Administraciones públicas desde una perspectiva global y no fragmentaria, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, en el ámbito de la Ley 11/2007, de 22 de junio, al objeto de conseguir un común denominador normativo.

En consecuencia, el Esquema Nacional de Interoperabilidad atiende a todos aquellos aspectos que conforman de manera global la interoperabilidad. En primer lugar, se atiende a las dimensiones organizativa, semántica y técnica a las que se refiere el artículo 41 de la Ley 11/2007, de 22 de junio; en segundo lugar, se tratan los estándares, que la Ley 11/2007, de 22 de junio, pone al servicio de la interoperabilidad así como de la independencia en la elección de las alternativas tecnológicas y del derecho de los ciudadanos a elegir las aplicaciones o sistemas para relacionarse con las Administraciones públicas; en tercer lugar, se tratan las infraestructuras y los servicios comunes, elementos reconocidos de dinamización, simplificación y propagación de la interoperabilidad, a la vez que facilitadores de la relación multilateral; en cuarto lugar, se trata la reutilización, aplicada a las aplicaciones

de las Administraciones públicas, de la documentación asociada y de otros objetos de información, dado que la voz «compartir» se encuentra presente en la definición de interoperabilidad recogida en la Ley 11/2007, de 22 de junio, y junto con «reutilizar», ambas son relevantes para la interoperabilidad y se encuentran entroncadas con las políticas de la Unión Europea en relación con la idea de compartir, reutilizar y colaborar; en quinto lugar, se trata la interoperabilidad de la firma electrónica y de los certificados; por último, se atiende a la conservación, según lo establecido en la citada Ley 11/2007,de 22 de junio, como manifestación de la interoperabilidad a lo largo del tiempo, y que afecta de forma singular al documento electrónico.

En esta norma se hace referencia a la interoperabilidad como un proceso integral, en el que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

La norma se estructura en doce capítulos, cuatro disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria, tres disposiciones finales y un anexo conteniendo el glosario de términos.

El Esquema Nacional de Interoperabilidad se remite al Esquema Nacional de Seguridad para las cuestiones relativas en materia de seguridad que vayan más allá de los aspectos necesarios para garantizar la interoperabilidad.

El presente real decreto se aprueba en aplicación de lo dispuesto en la disposición final octava de la Ley 11/2007, de 22 de junio y, de acuerdo con lo dispuesto en el artículo 42, apartado 3, y disposición final primera de dicha norma, se ha elaborado con la participación de todas las Administraciones Públicas a las que les es de aplicación, ha sido informado favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica, la Conferencia Sectorial de Administración Pública y la Comisión Nacional de Administración Local; y ha sido sometido al previo informe de la Agencia Española de Protección de Datos. Asimismo se ha sometido a la audiencia de los ciudadanos según las previsiones establecidas en el artículo 24 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

En su virtud, a propuesta de la Ministra de la Presidencia, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de enero de 2010,

DISPONGO:

CAPÍTULO I

**Disposiciones generales**

**Artículo 1.** *Objeto.*

1. El presente real decreto tiene por objeto regular el Esquema Nacional de Interoperabilidad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio.

2. El Esquema Nacional de Interoperabilidad comprenderá los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para evitar la discriminación a los ciudadanos por razón de su elección tecnológica.

**Artículo 2.** *Definiciones.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos se entenderán en el sentido indicado en el Glosario de Términos incluido en el anexo.

**Artículo 3.** *Ámbito de aplicación.*

1. El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.

2. El Esquema Nacional de Interoperabilidad y sus normas de desarrollo, prevalecerán sobre cualquier otro criterio en materia de política de interoperabilidad en la utilización de medios electrónicos para el acceso de los ciudadanos a los servicios públicos.

## CAPÍTULO II

## Principios básicos

**Artículo 4.** *Principios básicos del Esquema Nacional de Interoperabilidad.*

La aplicación del Esquema Nacional de Interoperabilidad se desarrollará de acuerdo con los principios generales establecidos en el artículo 4 de la Ley 11/2007, de 22 de junio, y con los siguientes principios específicos de la interoperabilidad:

a) La interoperabilidad como cualidad integral.
b) Carácter multidimensional de la interoperabilidad.
c) Enfoque de soluciones multilaterales.

**Artículo 5.** *La interoperabilidad como cualidad integral.*

La interoperabilidad se tendrá presente de forma integral desde la concepción de los servicios y sistemas y a lo largo de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión con los mismos.

**Artículo 6.** *Carácter multidimensional de la interoperabilidad.*

La interoperabilidad se entenderá contemplando sus dimensiones organizativa, semántica y técnica. La cadena de interoperabilidad se manifiesta en la práctica en los acuerdos interadministrativos, en el despliegue de los sistemas y servicios, en la determinación y uso de estándares, en las infraestructuras y servicios básicos de las Administraciones públicas y en la publicación y reutilización de las aplicaciones de las Administraciones públicas, de la documentación asociada y de otros objetos de información. Todo ello sin olvidar la dimensión temporal que ha de garantizar el acceso a la información a lo largo del tiempo.

**Artículo 7.** *Enfoque de soluciones multilaterales.*

Se favorecerá la aproximación multilateral a la interoperabilidad de forma que se puedan obtener las ventajas derivadas del escalado, de la aplicación de las arquitecturas modulares y multiplataforma, de compartir, de reutilizar y de colaborar.

## CAPÍTULO III

## Interoperabilidad organizativa

**Artículo 8.** *Servicios de las Administraciones públicas disponibles por medios electrónicos.*

1. Las Administraciones públicas establecerán y publicarán las condiciones de acceso y utilización de los servicios, datos y documentos en formato electrónico que pongan a disposición del resto de Administraciones especificando las finalidades, las modalidades de consumo, consulta o interacción, los requisitos que deben satisfacer los posibles usuarios de los mismos, los perfiles de los participantes implicados en la utilización de los servicios, los protocolos y criterios funcionales o técnicos necesarios para acceder a dichos servicios, los necesarios mecanismos de gobierno de los sistemas interoperables, así como las condiciones de seguridad aplicables. Estas condiciones deberán en todo caso resultar conformes a los principios, derechos y obligaciones contenidos en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de

desarrollo, así como a lo dispuesto en el Esquema Nacional de Seguridad, y los instrumentos jurídicos que deberán suscribir las Administraciones públicas requeridoras de dichos servicios, datos y documentos.

Se potenciará el establecimiento de convenios entre las Administraciones públicas emisoras y receptoras y, en particular, con los nodos de interoperabilidad previstos en el apartado 3 de este artículo, con el objetivo de simplificar la complejidad organizativa sin menoscabo de las garantías jurídicas.

Al objeto de dar cumplimiento de manera eficaz a lo establecido en el artículo 9 de la Ley 11/2007, de 22 de junio, en el Comité Sectorial de Administración electrónica se identificarán, catalogarán y priorizarán los servicios de interoperabilidad que deberán prestar las diferentes Administraciones públicas.

2. Las Administraciones públicas publicarán aquellos servicios que pongan a disposición de las demás administraciones a través de la Red de comunicaciones de las Administraciones públicas españolas, o de cualquier otra red equivalente o conectada a la misma que garantice el acceso seguro al resto de administraciones.

3. Las Administraciones públicas podrán utilizar nodos de interoperabilidad, entendidos como entidades a las cuales se les encomienda la gestión de apartados globales o parciales de la interoperabilidad organizativa, semántica o técnica.

**Artículo 9.** *Inventarios de información administrativa.*

1. Cada Administración Pública mantendrá actualizado el conjunto de sus inventarios de información administrativa que incluirá, al menos:

a) La relación de los procedimientos administrativos y servicios prestados de forma clasificada y estructurada. Las Administraciones Públicas conectarán electrónicamente sus inventarios con el Sistema de Información Administrativa gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital.

b) La relación de sus órganos administrativos y oficinas orientadas al público y sus relaciones entre ellos. Dicho inventario se conectará electrónicamente con el Directorio Común de Unidades Orgánicas y Oficinas, gestionado por el Ministerio de Asuntos Económicos y Transformación Digital, en colaboración con el Ministerio de Política Territorial y Función Pública, que proveerá una codificación unívoca.

2. Cada Administración Pública regulará la creación y mantenimiento de estos dos inventarios, en las condiciones que se determinen, con carácter general, por las normas técnicas de interoperabilidad correspondientes; en su caso, las Administraciones Públicas podrán hacer uso de los citados Sistema de Información Administrativa y Directorio Común de Unidades Orgánicas y Oficinas para la creación y mantenimiento de sus propios inventarios. Para la descripción y modelización de los procedimientos administrativos y de los procesos que los soportan será de aplicación lo previsto sobre estándares en el artículo 11.

## CAPÍTULO IV

## Interoperabilidad semántica

**Artículo 10.** *Activos semánticos.*

1. Se establecerá y mantendrá actualizada la Relación de modelos de datos de intercambio que tengan el carácter de comunes, que serán de preferente aplicación para los intercambios de información en las Administraciones públicas, de acuerdo con el procedimiento establecido en disposición adicional primera.

2. Los órganos de la Administración pública o Entidades de Derecho Público vinculadas o dependientes de aquélla, titulares de competencias en materias sujetas a intercambio de información con los ciudadanos y con otras Administraciones públicas, así como en materia de infraestructuras, servicios y herramientas comunes, establecerán y publicarán los correspondientes modelos de datos de intercambio que serán de obligatoria aplicación para los intercambios de información en las Administraciones públicas.

3. Los modelos de datos a los que se refieren los apartados 1 y 2, se ajustarán a lo previsto sobre estándares en el artículo 11 y se publicarán, junto con las definiciones y codificaciones asociadas, a través del Centro de Interoperabilidad Semántica de la Administración, según las condiciones de licenciamiento previstas en el artículo 16.

4. Las definiciones y codificaciones empleadas en los modelos de datos a los que se refieren los apartados anteriores tendrán en cuenta lo dispuesto en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y el resto de disposiciones que regulan la función estadística.

## CAPÍTULO V

## Interoperabilidad técnica

**Artículo 11.** *Estándares aplicables.*

1. Las Administraciones públicas usarán estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos, al objeto de garantizar la independencia en la elección de alternativas tecnológicas por los ciudadanos y las Administraciones públicas y la adaptabilidad al progreso de la tecnología y, de forma que:

a) Los documentos y servicios de administración electrónica que los órganos o Entidades de Derecho Público emisores pongan a disposición de los ciudadanos o de otras Administraciones públicas se encontrarán, como mínimo, disponibles mediante estándares abiertos.

b) Los documentos, servicios electrónicos y aplicaciones puestos por las Administraciones públicas a disposición de los ciudadanos o de otras Administraciones públicas serán, según corresponda, visualizables, accesibles y funcionalmente operables en condiciones que permitan satisfacer el principio de neutralidad tecnológica y eviten la discriminación a los ciudadanos por razón de su elección tecnológica.

2. En las relaciones con los ciudadanos y con otras Administraciones públicas, el uso en exclusiva de un estándar no abierto sin que se ofrezca una alternativa basada en un estándar abierto se limitará a aquellas circunstancias en las que no se disponga de un estándar abierto que satisfaga la funcionalidad satisfecha por el estándar no abierto en cuestión y sólo mientras dicha disponibilidad no se produzca. Las Administraciones públicas promoverán las actividades de normalización con el fin de facilitar la disponibilidad de los estándares abiertos relevantes para sus necesidades.

3. Para la selección de estándares, en general y, para el establecimiento del catálogo de estándares, en particular, se atenderá a los siguientes criterios:

a) El uso de las especificaciones técnicas de las TIC en la contratación pública junto con las definiciones de norma y especificación técnica establecidos en el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea.

b) La definición de estándar abierto establecida en la Ley 11/2007, de 22 de junio, anexo, letra k).

c) Carácter de especificación formalizada.

d) Definición de «coste que no suponga una dificultad de acceso», establecida en el anexo de este real decreto.

e) Consideraciones adicionales referidas a la adecuación del estándar a las necesidades y funcionalidad requeridas; a las condiciones relativas a su desarrollo, uso o implementación, documentación disponible y completa, publicación, y gobernanza del estándar; a las condiciones relativas a la madurez, apoyo y adopción del mismo por parte del mercado, a su potencial de reutilización, a la aplicabilidad multiplataforma y multicanal y a su implementación bajo diversos modelos de desarrollo de aplicaciones.

4. Para el uso de los estándares complementarios a la selección indicada en el apartado anterior, se tendrá en cuenta la definición de «uso generalizado por los ciudadanos» establecida en el anexo del presente real decreto.

5. En cualquier caso los ciudadanos podrán elegir las aplicaciones o sistemas para relacionarse con las Administraciones públicas, o dirigirse a las mismas, siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos. Para facilitar la interoperabilidad con las Administraciones públicas el catálogo de estándares contendrá una relación de estándares abiertos y en su caso complementarios aplicables.

## CAPÍTULO VI

## Infraestructuras y servicios comunes

**Artículo 12.** *Uso de infraestructuras y servicios comunes y herramientas genéricas.*

Las Administraciones públicas enlazarán aquellas infraestructuras y servicios que puedan implantar en su ámbito de actuación con las infraestructuras y servicios comunes que proporcione la Administración General del Estado para facilitar la interoperabilidad y la relación multilateral en el intercambio de información y de servicios entre todas las Administraciones públicas.

## CAPÍTULO VII

## Comunicaciones de las Administraciones públicas

**Artículo 13.** *Red de comunicaciones de las Administraciones públicas españolas.*

1. Al objeto de satisfacer lo previsto en el artículo 43 de la Ley 11/2007, de 22 de junio, las Administraciones públicas utilizarán preferentemente la Red de comunicaciones de las Administraciones públicas españolas para comunicarse entre sí, para lo cual conectarán a la misma, bien sus respectivas redes, bien sus nodos de interoperabilidad, de forma que se facilite el intercambio de información y de servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados miembros.

La Red SARA prestará la citada Red de comunicaciones de las Administraciones públicas españolas.

2. Para la conexión a la Red de comunicaciones de las Administraciones públicas españolas serán de aplicación los requisitos previstos en la disposición adicional primera.

**Artículo 14.** *Plan de direccionamiento de la Administración.*

Las Administraciones Públicas aplicarán el Plan de direccionamiento e interconexión de redes en la Administración, desarrollado en la norma técnica de interoperabilidad correspondiente, para su interconexión a través de las redes de comunicaciones.

**Artículo 15.** *Hora oficial.*

1. Los sistemas o aplicaciones implicados en la provisión de un servicio público por vía electrónica se sincronizarán con la hora oficial, con una precisión y desfase que garanticen la certidumbre de los plazos establecidos en el trámite administrativo que satisfacen.

2. La sincronización de la fecha y la hora se realizará con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al Centro Español de Metrología y, cuando sea posible, con la hora oficial a nivel europeo.

CAPÍTULO VIII

**Reutilización y transferencia de tecnología**

**Artículo 16.** *Condiciones de licenciamiento aplicables.*

1. Las condiciones de licenciamiento de las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información cuya titularidad de los derechos de la propiedad intelectual sea de una Administración Pública y permita su puesta a disposición de otra Administración y de los ciudadanos tendrán en cuenta los siguientes aspectos:

a) El fin perseguido es el aprovechamiento y la reutilización de recursos públicos.
b) La completa protección contra su apropiación exclusiva o parcial por parte de terceros.
c) La exención de responsabilidad del cedente por el posible mal uso por parte del cesionario.
d) La no obligación de asistencia técnica o de mantenimiento por parte del cedente.
e) La ausencia total de responsabilidad por parte del cedente con respecto al cesionario en caso de errores o mal funcionamiento de la aplicación.
f) El licenciamiento se realizará por defecto sin contraprestación y sin necesidad de establecer convenio alguno. Sólo se podrá acordar la repercusión parcial del coste de adquisición o desarrollo de las aplicaciones cedidas en aquellos casos en los que este pago repercuta directamente en el incremento de funcionalidades del activo cedido, incluya adaptaciones concretas para su uso en el organismo cesionario, o impliquen el suministro de servicios de asistencia o soporte para su reutilización en el organismo cesionario.

2. Las Administraciones Públicas utilizarán para las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información declarados como de fuentes abiertas aquellas licencias que aseguren que los programas, datos o información cumplen los siguientes requisitos:

a) Pueden ejecutarse para cualquier propósito.
b) Permiten conocer su código fuente.
c) Pueden modificarse o mejorarse.
d) Pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas cuatro garantías.

3. Para este fin se procurará la aplicación de la Licencia Pública de la Unión Europea, sin perjuicio de otras licencias que garanticen los mismos derechos expuestos en los apartados 1 y 2.
4. A efectos de facilitar el establecimiento de las condiciones de licenciamiento, las Administraciones Públicas incluirán en los pliegos de cláusulas técnicas de aquellos contratos que tengan por finalidad el desarrollo de nuevas aplicaciones informáticas, los siguientes aspectos:

a) Que la Administración contratante adquiera los derechos completos de propiedad intelectual de las aplicaciones y cualquier otro objeto de información que se desarrollen como objeto de ese contrato.
b) Que en el caso de reutilizar activos previamente existentes, la Administración contratante reciba un producto que pueda ofrecer para su reutilización posterior a otras Administraciones Públicas. Además, en el caso de partir de productos de fuentes abiertas, que sea posible declarar como de fuentes abiertas la futura aplicación desarrollada.

**Artículo 17.** *Directorios de aplicaciones reutilizables.*

1. La Administración General del Estado mantendrá el Directorio general de aplicaciones para su libre reutilización, de acuerdo al artículo 158 de la Ley 40/2015, de 1 octubre, a través del Centro de Transferencia de Tecnología. Este directorio podrá ser utilizado por otras Administraciones Públicas. En el caso de disponer de un directorio propio, deberá garantizar que las aplicaciones disponibles en ese directorio propio se pueden consultar también a través del Centro de Transferencia de Tecnología.
2. Las Administraciones Públicas conectarán los directorios de aplicaciones para su libre reutilización entre sí; y con instrumentos equivalentes del ámbito de la Unión Europea.

3. Las Administraciones Públicas publicarán las aplicaciones reutilizables, en modo producto o en modo servicio, en los directorios de aplicaciones para su libre reutilización, con al menos el siguiente contenido:

a) Código fuente de las aplicaciones finalizadas, en el caso de ser reutilizables en modo producto y haber sido declaradas de fuentes abiertas.
b) Documentación asociada.
c) Condiciones de licenciamiento de todos los activos, en el caso de ser reutilizables en modo producto, o nivel de servicio ofrecido, en el caso de ser reutilizables en modo servicio.
d) Los costes asociados a su reutilización, en el caso de que existieran.

4. Las Administraciones procurarán la incorporación a la aplicación original de aquellas modificaciones o adaptaciones realizadas sobre cualquier aplicación que se haya obtenido desde un directorio de aplicaciones reutilizables.

## CAPÍTULO IX

## Firma electrónica y certificados

**Artículo 18.** *Interoperabilidad en la política de firma electrónica y de certificados.*

1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para el reconocimiento mutuo de las firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Públicas.

Todos los organismos y entidades de derecho público de la Administración General del Estado aplicarán la política de firma electrónica y de certificados a que se refiere el párrafo anterior. La no aplicación de dicha política deberá ser justificada por el órgano u organismo competente y autorizada por la Secretaría General de Administración Digital.

2. Las restantes Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados a que hace referencia el apartado anterior.

3. Sin perjuicio de lo expuesto en el apartado anterior, las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales.

Las políticas de firma electrónica que aprueben las Administraciones Públicas partirán de la norma técnica establecida a tal efecto en la disposición adicional primera, de los estándares técnicos existentes, y deberán ser interoperables con la política marco de firma electrónica mencionada en el apartado 1, en particular, con sus ficheros de implementación. La Administración Pública proponente de una política de firma electrónica particular garantizará su interoperabilidad con la citada política marco de firma electrónica y con sus correspondientes ficheros de implementación según las condiciones establecidas en la norma técnica de interoperabilidad recogida a tal efecto en la disposición adicional primera.

4. Al objeto de garantizar la interoperabilidad de las firmas electrónicas emitidas conforme a las políticas establecidas, las políticas de firma electrónica que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

5. Las Administraciones Públicas receptoras de documentos electrónicos firmados, siempre que hayan admitido con anterioridad la política de firma del emisor, permitirán la validación de las firmas electrónicas según la política de firma indicada en la firma del documento electrónico.

6. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones Públicas sin ningún tipo de restricción técnica, semántica u organizativa.

7. Los procedimientos en los que se utilicen certificados de firma electrónica deberán atenerse a la política de firma electrónica y de certificados aplicable en su ámbito, particularmente en la aplicación de los datos obligatorios y opcionales, las reglas de creación

y validación de firma electrónica, los algoritmos a utilizar y longitudes de clave mínimas aplicables.

**Artículo 19.** *Aspectos de interoperabilidad relativos a los prestadores de servicios de certificación.*

**(Suprimido)**

**Artículo 20.** *Plataformas de validación de certificados electrónicos y de firma electrónica.*

1. Las plataformas de validación de certificados electrónicos y de firma electrónica proporcionarán servicios de confianza a las aplicaciones usuarias o consumidoras de los servicios de certificación y firma, proporcionando servicios de validación de los certificados y firmas generadas y admitidas en diversos ámbitos de las Administraciones públicas.

2. Proporcionarán, en un único punto de llamada, todos los elementos de confianza y de interoperabilidad organizativa, semántica y técnica necesarios para integrar los distintos certificados reconocidos y firmas que pueden encontrase en los dominios de dos administraciones diferentes.

3. Potenciarán la armonización técnica y la utilización común de formatos, estándares y políticas de firma electrónica y de certificados para las firmas electrónicas entre las aplicaciones usuarias, y de otros elementos de interoperabilidad relacionados con los certificados, tales como el análisis de los campos y extracción univoca de la información pertinente. En particular, se tendrán en cuenta los estándares europeos de las Organizaciones Europeas de Estandarización en el campo de las Tecnologías de Información y Comunicación aplicadas a la firma electrónica.

4. Incorporarán las listas de confianza de los certificados interoperables entre las distintas Administraciones públicas nacionales y europeas según el esquema operativo de gestión correspondiente de la lista de confianza.

## CAPÍTULO X

## Recuperación y conservación del documento electrónico

**Artículo 21.** *Condiciones para la recuperación y conservación de documentos.*

1. Las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Tales medidas incluirán:

a) La definición de una política de gestión de documentos en cuanto al tratamiento, de acuerdo con las normas y procedimientos específicos que se hayan de utilizar en la formación y gestión de los documentos y expedientes.

b) La inclusión en los expedientes de un índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del expediente electrónico y permita su recuperación.

c) La identificación única e inequívoca de cada documento por medio de convenciones adecuadas, que permitan clasificarlo, recuperarlo y referirse al mismo con facilidad.

d) La asociación de los metadatos mínimos obligatorios y, en su caso, complementarios, asociados al documento electrónico, a lo largo de su ciclo de vida, e incorporación al esquema de metadatos.

e) La clasificación, de acuerdo con un plan de clasificación adaptado a las funciones, tanto generales como específicas, de cada una de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas.

f) El período de conservación de los documentos, establecido por las comisiones calificadoras que correspondan, de acuerdo con la legislación en vigor, las normas administrativas y obligaciones jurídicas que resulten de aplicación en cada caso.

g) El acceso completo e inmediato a los documentos a través de métodos de consulta en línea que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los

formatos originales y la impresión a papel de aquellos documentos que sean necesarios. El sistema permitirá la consulta durante todo el período de conservación al menos de la firma electrónica, incluido, en su caso, el sello de tiempo, y de los metadatos asociados al documento.

h) La adopción de medidas para asegurar la conservación de los documentos electrónicos a lo largo de su ciclo de vida, de acuerdo con lo previsto en el artículo 22, de forma que se pueda asegurar su recuperación de acuerdo con el plazo mínimo de conservación determinado por las normas administrativas y obligaciones jurídicas, se garantice su conservación a largo plazo, se asegure su valor probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos, así como la transparencia, la memoria y la identificación de los órganos de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas que ejercen la competencia sobre el documento o expediente.

i) La coordinación horizontal entre el responsable de gestión de documentos y los restantes servicios interesados en materia de archivos.

j) Transferencia, en su caso, de los expedientes entre los diferentes repositorios electrónicos a efectos de conservación, de acuerdo con lo establecido en la legislación en materia de Archivos, de manera que se pueda asegurar su conservación, y recuperación a medio y largo plazo.

k) Si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación.

l) La formación tecnológica del personal responsable de la ejecución y del control de la gestión de documentos, como de su tratamiento y conservación en archivos o repositorios electrónicos.

m) La documentación de los procedimientos que garanticen la interoperabilidad a medio y largo plazo, así como las medidas de identificación, recuperación, control y tratamiento de los documentos electrónicos.

2. A los efectos de lo dispuesto en el apartado 1, las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos.

**Artículo 22.** *Seguridad.*

1. Para asegurar la conservación de los documentos electrónicos se aplicará lo previsto en el Esquema Nacional de Seguridad en cuanto al cumplimento de los principios básicos y de los requisitos mínimos de seguridad mediante la aplicación de las medidas de seguridad adecuadas a los medios y soportes en los que se almacenen los documentos, de acuerdo con la categorización de los sistemas.

2. Cuando los citados documentos electrónicos contengan datos de carácter personal les será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo.

3. Estas medidas se aplicarán con el fin de garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios, y se realizarán atendiendo a los riesgos a los que puedan estar expuestos y a los plazos durante los cuales deban conservarse los documentos.

4. Los aspectos relativos a la firma electrónica en la conservación del documento electrónico se establecerán en la Política de firma electrónica y de certificados, y a través del uso de formatos de firma longeva que preserven la conservación de las firmas a lo largo del tiempo.

Cuando la firma y los certificados no puedan garantizar la autenticidad y la evidencia de los documentos electrónicos a lo largo del tiempo, éstas les sobrevendrán a través de su conservación y custodia en los repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos.

**Artículo 23.** *Formatos de los documentos.*

1. Con el fin de garantizar la conservación, el documento se conservará en el formato en que haya sido elaborado, enviado o recibido, y preferentemente en un formato correspondiente a un estándar abierto que preserve a lo largo del tiempo la integridad del contenido del documento, de la firma electrónica y de los metadatos que lo acompañan.

2. La elección de formatos de documento electrónico normalizados y perdurables para asegurar la independencia de los datos de sus soportes se realizará de acuerdo con lo previsto en el artículo 11.

3. Cuando exista riesgo de obsolescencia del formato o bien deje de figurar entre los admitidos en el presente Esquema Nacional de Interoperabilidad, se aplicarán procedimientos normalizados de copiado auténtico de los documentos con cambio de formato, de etiquetado con información del formato utilizado y, en su caso, de las migraciones o conversiones de formatos.

**Artículo 24.** *Digitalización de documentos en soporte papel.*

1. La digitalización de documentos en soporte papel por parte de las Administraciones públicas se realizará de acuerdo con lo indicado en la norma técnica de interoperabilidad correspondiente en relación con los siguientes aspectos:

a) Formatos estándares de uso común para la digitalización de documentos en soporte papel y técnica de compresión empleada, de acuerdo con lo previsto en el artículo 11.

b) Nivel de resolución.

c) Garantía de imagen fiel e íntegra.

d) Metadatos mínimos obligatorios y complementarios, asociados al proceso de digitalización.

2. La gestión y conservación del documento electrónico digitalizado atenderá a la posible existencia del mismo en otro soporte.

CAPÍTULO XI

**Normas de conformidad**

**Artículo 25.** *Sedes y registros electrónicos.*

La interoperabilidad de las sedes y registros electrónicos, así como la del acceso electrónico de los ciudadanos a los servicios públicos, se regirán por lo establecido en el Esquema Nacional de Interoperabilidad.

**Artículo 26.** *Ciclo de vida de servicios y sistemas.*

La conformidad con el Esquema Nacional de Interoperabilidad se incluirá en el ciclo de vida de los servicios y sistemas, acompañada de los correspondientes procedimientos de control.

**Artículo 27.** *Mecanismo de control.*

Cada órgano o Entidad de Derecho Público establecerá sus mecanismos de control para garantizar, de forma efectiva, el cumplimiento del Esquema Nacional de Interoperabilidad.

**Artículo 28.** *Publicación de conformidad.*

Los órganos y Entidades de Derecho Público de las Administraciones públicas darán publicidad, en las correspondientes sedes electrónicas, a las declaraciones de conformidad y a otros posibles distintivos de interoperabilidad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Interoperabilidad.

CAPÍTULO XII

**Actualización**

**Artículo 29.** *Actualización permanente.*

El Esquema Nacional de Interoperabilidad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que le apoyan.

**Disposición adicional primera.** *Desarrollo del Esquema Nacional de Interoperabilidad.*

1. Se desarrollarán las siguientes normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones Públicas:

a) Norma Técnica de Catálogo de estándares: establecerá un conjunto de estándares que satisfagan lo previsto en el artículo 11 de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados.

b) Norma Técnica de Documento electrónico: tratará los metadatos mínimos obligatorios, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados; y los formatos de documento.

c) Norma Técnica de Digitalización de documentos: tratará los formatos y estándares aplicables, los niveles de calidad, las condiciones técnicas y los metadatos asociados al proceso de digitalización.

d) Norma Técnica de Expediente electrónico: tratará de su estructura y formato, así como de las especificaciones de los servicios de remisión y puesta a disposición.

e) Norma Técnica de Política de firma electrónica y de certificados de la Administración: Tratará, entre otras cuestiones recogidas en su definición en el anexo, aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones Públicas.

f) Norma Técnica de Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en las Administraciones Públicas y que serán de aplicación para los prestadores y consumidores de tales servicios.

g) Norma Técnica de Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras Administraciones.

h) Norma Técnica de Política de gestión de documentos electrónicos: incluirá directrices para la asignación de responsabilidades, tanto directivas como profesionales, y la definición de los programas, procesos y controles de gestión de documentos y administración de los repositorios electrónicos, y la documentación de los mismos, a desarrollar por las Administraciones Públicas y por los organismos públicos y entidades de derecho público vinculados o dependientes de aquéllas.

i) Norma Técnica de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas.

j) Norma Técnica de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.

k) Norma Técnica de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales: tratará de aspectos funcionales y técnicos para el intercambio de asientos registrales, gestión de errores y excepciones, gestión de anexos, requerimientos tecnológicos y transformaciones de formatos.

l) Norma Técnica de Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de información puestos a disposición del público por medios electrónicos para su reutilización.

m) Norma Técnica de interoperabilidad de inventario y codificación de objetos administrativos: tratará las reglas relativas a la codificación de objetos administrativos, así como la conexión entre los inventarios correspondientes, incluyendo, por un lado, las unidades orgánicas y oficinas de la Administración, y, por otro lado, la información administrativa de procedimientos y servicios.

n) Norma Técnica de Interoperabilidad de Transferencia e Ingreso de documentos y expedientes electrónicos: tratará los requisitos y condiciones relativos a la transferencia de agrupaciones documentales en formato electrónico, documentos y expedientes electrónicos, junto con los metadatos asociados, entre sistemas de gestión de documentos electrónicos y sistemas de archivo electrónico.

ñ) Norma Técnica de Interoperabilidad de Valoración y Eliminación de documentos y expedientes electrónicos: tratará las condiciones y requisitos relativos a la valoración de los documentos y expedientes electrónicos para establecimiento de plazos de conservación, transferencia y acceso o, en su caso, eliminación total o parcial.

o) Norma Técnica de Interoperabilidad de preservación de documentación electrónica: tratará las condiciones y requisitos relativos a la conservación de los documentos electrónicos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, así como la protección, recuperación y conservación física y lógica de los documentos y su contexto.

p) Norma Técnica de Interoperabilidad de tratamiento y preservación de bases de datos: tratará las condiciones y requisitos relativos a la conservación de las bases de datos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, y permitiendo la protección, recuperación y conservación física y lógica de los datos y su contexto.

q) Norma Técnica de Interoperabilidad de Plan de Direccionamiento: tratará reglas aplicables a la asignación y requisitos de direccionamiento IP para garantizar la correcta administración de la Red de comunicaciones de las Administraciones Públicas españolas y evitar el uso de direcciones duplicadas.

r) Norma Técnica de Interoperabilidad de reutilización de activos en modo producto y en modo servicio: tratará los requisitos y condiciones para facilitar la reutilización de activos tanto en modo producto como en modo servicio por las Administraciones Públicas españolas.

s) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros de funcionarios habilitados: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de funcionarios habilitados pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas.

t) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros electrónicos de apoderamientos: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, A los registros mercantiles, de la propiedad, y a los protocolos notariales.

u) Norma Técnica de Interoperabilidad de Sistema de Referencia de documentos y repositorios de confianza: tratará los requisitos técnicos que deberán cumplir las referencias a documentos al ser intercambiadas, de forma que se evite trasladar documentación de forma innecesaria.

v) Norma Técnica de Política de firma electrónica y de certificados en el ámbito estatal: tratará las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación, organizadas alrededor de los conceptos de generación y validación de firma e incluirá los perfiles interoperables de los medios de identificación de las Administraciones Públicas previstos en Ley 40/2015, de 1 de octubre.

2. El Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica prevista en la disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, aprobará las normas técnicas de interoperabilidad y las publicará mediante Resolución de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

3. Para la redacción y actualización de las normas técnicas de interoperabilidad indicadas en el apartado 1 y las futuras que pueda aprobar el Ministerio de Asuntos Económicos y Transformación Digital que sean necesarias para garantizar el adecuado nivel de interoperabilidad como consecuencia del nivel de desarrollo tecnológico, los compromisos internacionales o el marco normativo aplicable, se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de Administración electrónica.

Para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, el órgano competente será el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia.

4. Se desarrollarán los siguientes instrumentos para la interoperabilidad:

a) Sistema de Información Administrativa: Inventario de procedimientos administrativos, servicios prestados y otras actuaciones administrativas que generen documentación pública, conteniendo información de los mismos clasificada por funciones y con indicación de su nivel de informatización, así como información acerca de las interfaces al objeto de favorecer la interacción o en su caso la integración de los procesos.

b) Centro de interoperabilidad semántica de la Administración: Almacenará, publicará y difundirá los modelos de datos de los servicios de interoperabilidad entre Administraciones Públicas y de estas con los ciudadanos, tanto comunes como sectoriales, así como los relativos a infraestructuras y servicios comunes, además de las especificaciones semánticas y codificaciones relacionadas. Su propósito es facilitar la comprensión semántica de los servicios de intercambio de datos de las Administraciones y maximizar la reutilización de activos semánticos en la construcción de éstos. Se conectará con otros instrumentos equivalentes de las Administraciones Públicas y del ámbito de la Unión Europea.

c) Centro de Transferencia de Tecnología: Directorio de aplicaciones para su libre reutilización que contendrá la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

d) Directorio Común de Unidades Orgánicas y Oficinas de las Administraciones Públicas: Instrumento que permitirá la sincronización de los sistemas que traten la información de inventariado, codificación y evolución de unidades orgánicas y oficinas en diferentes modalidades de integración para garantizar la flexibilidad tanto en el consumo como en la provisión de información relacionada.

**Disposición adicional segunda.** *Formación.*

El personal de las Administraciones públicas recibirá la formación necesaria para garantizar el conocimiento del presente Esquema Nacional de Interoperabilidad, a cuyo fin los órganos responsables dispondrán lo necesario para que esta formación sea una realidad efectiva.

**Disposición adicional tercera.** *Centro Nacional de Referencia de Aplicación de las Tecnologías de la Información y la Comunicación (TIC) basadas en fuentes abiertas.*

**(Suprimida)**

**Disposición adicional cuarta.** *Instituto Nacional de Tecnologías de la Comunicación.*

**(Suprimida)**

**Disposición adicional quinta.** *Normativa técnica relativa a la reutilización de recursos de información.*

La normativa relativa a la reutilización de recursos de información deberá estar aprobada a más tardar el 1 de junio de 2012.

**Disposición transitoria primera.** *Adecuación de sistemas y servicios.*

Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Interoperabilidad de forma que permitan el cumplimiento de lo establecido en la Disposición final tercera de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.

Si a los doce meses de la entrada en vigor del Esquema Nacional de Interoperabilidad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación, que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

**Disposición transitoria segunda.** *Uso de medios actualmente admitidos de identificación y autenticación.*

De acuerdo con lo previsto en el artículo 19 de la Ley 11/2007, de 22 de junio, y en la disposición transitoria primera del Real Decreto 1671/2009, de 6 de noviembre, se establece un plazo de adaptación de veinticuatro meses en el que se podrá seguir utilizando los medios actualmente admitidos de identificación y firma electrónica.

**Disposición derogatoria única.**

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en el presente reglamento.

**Disposición final primera.** *Título habilitante.*

El presente real decreto se dicta en virtud de lo establecido en el artículo 149.1.18.ª de la Constitución, que atribuye al Estado la competencia sobre las bases del régimen jurídico de las Administraciones Públicas.

**Disposición final segunda.** *Desarrollo normativo.*

Se autoriza al titular del Ministerio de la Presidencia, para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

**Disposición final tercera.** *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## ANEXO

### Glosario de términos

Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática.

Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otros usuarios.

Cadena de interoperabilidad: Expresión de la interoperabilidad en el despliegue de los sistemas y los servicios como una sucesión de elementos enlazados e interconectados, de forma dinámica, a través de interfaces y con proyección a las dimensiones técnica, semántica y organizativa.

Ciclo de vida de un documento electrónico: Conjunto de las etapas o períodos por los que atraviesa la vida del documento, desde su identificación en un sistema de gestión de

documentos, hasta su selección para conservación permanente, de acuerdo con la legislación sobre Archivos de aplicación en cada caso, o para su destrucción reglamentaria.

Coste que no suponga una dificultad de acceso: Precio del estándar que, por estar vinculado al coste de distribución y no a su valor, no impide conseguir su posesión o uso.

Dato: Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para comunicación, interpretación o procesamiento por medios automáticos o humanos.

Digitalización: El proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento.

Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Especificación técnica: Una especificación que figura en un documento en el que se definen las características requeridas de un producto, tales como los niveles de calidad, el uso específico, la seguridad o las dimensiones, incluidas las prescripciones aplicables al producto en lo referente a la denominación de venta, la terminología, los símbolos, los ensayos y métodos de ensayo, el envasado, el marcado y el etiquetado, así como los procedimientos de evaluación de la conformidad.

Especificación formalizada: Aquellas especificaciones que o bien son normas en el sentido de la Directiva 98/34 o bien proceden de consorcios de la industria u otros foros de normalización.

Esquema de metadatos: Instrumento que define la incorporación y gestión de los metadatos de contenido, contexto y estructura de los documentos electrónicos a lo largo de su ciclo de vida.

Estándar: Véase norma.

Estándar abierto: Aquél que reúne las siguientes condiciones:

a) Que sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,

b) Que su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

Ficheros de implementación de las políticas de firma: Son la representación en lenguaje formal (XML o ASN.1) de las condiciones establecidas en la política de firma, acorde a las normas técnicas establecidas por los organismos de estandarización.

Firma electrónica: Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Formato: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria.

Herramientas genéricas: Instrumentos y programas de referencia, compartidos, de colaboración o componentes comunes y módulos similares reutilizables que satisfacen las necesidades comunes en los distintos ámbitos administrativos.

Imagen electrónica: Resultado de aplicar un proceso de digitalización a un documento.

Índice electrónico: Relación de documentos electrónicos de un expediente electrónico, firmada por la Administración, órgano o entidad actuante, según proceda y cuya finalidad es garantizar la integridad del expediente electrónico y permitir su recuperación siempre que sea preciso.

Infraestructura o servicio común: capacidad organizativa y técnica que satisface necesidades comunes de los usuarios en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.

Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

Interoperabilidad organizativa: Es aquella dimensión de la interoperabilidad relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus

actividades para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan.

Interoperabilidad semántica: Es aquella dimensión de la interoperabilidad relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación.

Interoperabilidad técnica: Es aquella dimensión de la interoperabilidad relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga.

Interoperabilidad en el tiempo: Es aquella dimensión de la interoperabilidad relativa a la interacción entre elementos que corresponden a diversas oleadas tecnológicas; se manifiesta especialmente en la conservación de la información en soporte electrónico.

Licencia Pública de la Unión Europea («European Union Public Licence-EUPL»): Licencia adoptada oficialmente por la Comisión Europea en las 22 lenguas oficiales comunitarias para reforzar la interoperabilidad de carácter legal mediante un marco colectivo para la puesta en común de las aplicaciones del sector público.

Lista de servicios de confianza (TSL): Lista de acceso público que recoge información precisa y actualizada de aquellos servicios de certificación y firma electrónica que se consideran aptos para su empleo en un marco de interoperabilidad de las Administraciones públicas españolas y europeas.

Marca de tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

Modelo de datos: Conjunto de definiciones (modelo conceptual), interrelaciones (modelo lógico) y reglas y convenciones (modelo físico) que permiten describir los datos para su intercambio.

Nivel de resolución: Resolución espacial de la imagen obtenida como resultado de un proceso de digitalización.

Nodo de interoperabilidad: Organismo que presta servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones Públicas bajo las condiciones que éstas fijen.

Norma: Especificación técnica aprobada por un organismo de normalización reconocido para una aplicación repetida o continuada cuyo cumplimiento no sea obligatorio y que esté incluida en una de las categorías siguientes:

a) norma internacional: norma adoptada por una organización internacional de normalización y puesta a disposición del público,

b) norma europea: norma adoptada por un organismo europeo de normalización y puesta a disposición del público,

c) norma nacional: norma adoptada por un organismo nacional de normalización y puesta a disposición del público.

Política de firma electrónica: Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La

política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

Procedimiento administrativo: Proceso formal regulado jurídicamente para la toma de decisiones por parte de las Administraciones públicas para garantizar la legalidad, eficacia, eficiencia, calidad, derechos e intereses presentes, que termina con una resolución en la que se recoge un acto administrativo; este proceso formal jurídicamente regulado se implementa en la práctica mediante un proceso operativo que coincide en mayor o menor medida con el formal.

Proceso operativo: Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Repositorio electrónico: Archivo centralizado donde se almacenan y administran datos y documentos electrónicos, y sus metadatos.

Sello de tiempo: La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

Servicio de interoperabilidad: Cualquier mecanismo que permita a las Administraciones públicas compartir datos e intercambiar información mediante el uso de las tecnologías de la información.

Soporte: Objeto sobre el cual o en el cual es posible grabar y recuperar datos.

Trámite: Cada uno de los estados y diligencias que hay que recorrer en un negocio hasta su conclusión.

Uso generalizado por los ciudadanos: Usado por casi todas las personas físicas, personas jurídicas y entes sin personalidad que se relacionen o sean susceptibles de relacionarse con las Administraciones públicas españolas.

# § 13

## Resolución de 3 de octubre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 262, de 31 de octubre de 2012
Última modificación: sin modificaciones
Referencia: BOE-A-2012-13501

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, el Catálogo de estándares persigue facilitar que los servicios de Administración Electrónica puedan prestarse en condiciones que permitan la independencia en la elección de alternativas tecnológicas por los ciudadanos y las Administraciones públicas, así como la adaptabilidad al progreso de las técnicas y sistemas de comunicaciones descrito en la Ley 11/2007. Su desarrollo responde a las condiciones establecidas en el Real Decreto 4/2010, de 8 de enero, sobre estándares aplicables y se ciñe estrictamente a la finalidad de encontrarse al servicio de la interoperabilidad.

Para este fin, la Norma Técnica de Interoperabilidad de Catálogo de estándares establece un catálogo formado por un conjunto mínimo de estándares que satisfacen lo previsto en el artículo 11 del Real Decreto 4/2010, de 8 de enero, y que dan soporte al resto de Normas Técnicas de Interoperabilidad; asimismo establece condiciones necesarias para su revisión y actualización. Atendiendo a lo anterior, el uso de estándares no incluidos en esta norma respondería a necesidades específicas que igualmente aplicarían lo establecido en dicho artículo 11.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones Públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Catálogo de estándares que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la Disposición Transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

## NORMA TÉCNICA DE INTEROPERABILIDAD DE CATÁLOGO DE ESTÁNDARES

### I. Objeto

La Norma Técnica de Interoperabilidad de Catálogo de estándares tiene por objeto establecer un conjunto de estándares que satisfagan lo previsto en el artículo 11 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

### II. Ámbito de aplicación

Esta norma será de aplicación en el ámbito establecido en el artículo 3 del citado Real Decreto 4/2010, de 8 de enero.

### III. Catálogo de estándares

El Catálogo de estándares:

a) Incluirá el conjunto de estándares definido en el anexo estructurado conforme a diferentes categorías.

b) Atenderá a la aplicación de los criterios establecidos en el artículo 11 del Real Decreto 4/2010, de 8 de enero.

c) Recogerá los estándares mínimos necesarios para la interoperabilidad y para la implementación del resto de Normas Técnicas de Interoperabilidad.

d) Indicará para cada estándar el estado que le corresponde dentro del ciclo de vida, siendo los valores aplicables «Admitido» y «En abandono».

### IV. Uso de los estándares

Cada órgano de la Administración o Entidad de Derecho Público vinculada o dependiente de aquella:

a) Seleccionará, entre los establecidos en esta norma, el estándar o estándares que mejor se ajuste a sus necesidades, en base a su especificidad para la tarea o funcionalidad a cubrir, para los documentos y servicios que pongan a disposición de los ciudadanos o de otras Administraciones públicas, atendiendo a las condiciones establecidas en el artículo 11 del Real Decreto 4/2010, de 8 de enero.

Si una determinada funcionalidad o necesidad no quedara cubierta por ningún estándar de los recogidos en esta norma, podrá seleccionar el estándar más adecuado para la tarea atendiendo a lo establecido en artículo 11.2 del Real Decreto 4/2010, de 8 de enero. En este caso, informará del estándar seleccionado según lo establecido en el apartado V.2 de esta norma.

b) Para la interacción con otras administraciones, atenderá a los estándares seleccionados por el emisor del documento solicitado o responsable del servicio al que se desea acceder, que éste publicará según lo establecido en el artículo 8 del Real Decreto 4/2010, de 8 de enero. Dicha selección de estándares se realizará atendiendo a las condiciones establecidas en el artículo 11 del citado Real Decreto.

c) Publicará, según lo establecido en la normativa aplicable en cada caso, los estándares seleccionados para los servicios o trámites que ponga a disposición del ciudadano.

d) Podrá utilizar otros formatos cuando existan particularidades que lo justifiquen o sea necesario para asegurar el valor probatorio de la información electrónica de las actividades y procedimientos en caso de proceder a su conversión de formato.

### V. Revisión y actualización del Catálogo de estándares

1. La actualización y revisión del Catálogo de estándares se realizará con periodicidad anual, atenderá a los principios establecidos en el artículo 11 del Real Decreto 4/2010 e incluirá, al menos, las siguientes acciones:

a) Encuesta a las Administraciones públicas sobre el uso de los diferentes estándares del Catálogo.

b) Valoración y, si procede, eliminación de los estándares cuyo estado fuese «En abandono». Esta situación conllevará la selección de un estándar que sustituya la funcionalidad cubierta por el estándar eliminado.

c) Revisión del resto de estándares, así como de sus versiones, recogidos en el Catálogo a la fecha de la revisión de la misma, actualización, para aquellos que así lo requiriesen e identificación de los estándares en estado «En abandono», en cuyo caso se definirá un período máximo de uso.

d) Identificación de nuevos estándares a incluir en el Catálogo.

e) Valoración de nuevas necesidades o funcionalidades que no puedan catalogarse según la clasificación establecida y, si corresponde, modificación de las categorías y actualización del Catálogo de estándares en base a ésta.

2. En los casos necesarios, se podrá solicitar la actualización del Catálogo de estándares mediante petición formal a la Secretaría Ejecutiva del Comité Sectorial de Administración Electrónica, para decisión del mismo, que incluirá:

a) Tipo de solicitud: alta, modificación o baja de un estándar.
b) Datos a actualizar del estándar.
c) Razón de la actualización.

### ANEXO

### Catálogo de estándares

La tabla que figura a continuación recoge el conjunto de estándares incluidos en el Catálogo.

Para cada uno de ellos, se incluyen los siguientes atributos:

a) Cadena de interoperabilidad: eslabón de la cadena de interoperabilidad con el que se relaciona:

– Accesibilidad multicanal, integrada y segura.
– Infraestructuras y servicios asociados.
– Integración de sistemas y servicios.
– Modelos e integración de datos.

b) Categoría: Definición de la categoría funcional en la que se enmarca:

– Autenticación:

Certificados.
Firma electrónica.
Política de firma electrónica.

– Sellado de tiempo.
– Cifrado.

– Codificación:

Codificación de caracteres.
Idioma.

– Control de acceso.
– Formatos ficheros:

Imagen y/o texto.
Cartografía vectorial y sistemas de información geográfica.
Compresión de ficheros.
Contenedores multimedia.
Sonido.
Vídeo.

– Gestión documental y archivística.
– Integridad.
– Métricas.
– Protocolos de comunicación e intercambio:

Correo electrónico.
Específicos a nivel de aplicación.
Servicios Web.
Tecnologías de transporte y red.

– Semántica:

Metadatos.
Tecnologías semánticas.

– Tecnologías de integración de datos.
– Tecnologías de identificación.

c) Nombre:

– Común: nombre común por el que se conoce el estándar, normalmente identificado por su extensión. Define el valor a asignar al metadato mínimo obligatorio «Nombre de formato» de los documentos electrónicos.
– Formal: nombre correspondiente a la especificación formal del estándar.

d) Tipo:

– Estándar abierto.
– Uso generalizado.

e) Versión: versión mínima aceptada del estándar.

f) Extensión: Con carácter informativo, aproximación al listado no exhaustivo de extensiones más comunes relacionadas con el estándar.

g) Estado:

– Admitido.

– En abandono.

| Cadena de Interoperabilidad | Categoría | Nombre | | Tipo | | Versión (mínima aceptada) | Extensión | Estado |
|---|---|---|---|---|---|---|---|---|
| | | Común | Formal | | | | | |
| Accesibilidad multicanal, integrada y segura | Autenticación–Firma electrónica | CAdES | ETSI TS 101 733 Electronic Signatures and Infrastructures (ESO; CMS Advanced Electronic Signatures (CAdES) | Abierto | | 1.6.3 | .p7s .csig | Admitido |
| Accesibilidad multicanal, integrada y segura. | Autenticación - Firma electrónica | CMS | Cryptographic Message Syntax (CMS) | Abierto | | RFC 5652 | .sig | Admitido |
| Accesibilidad multicanal, integrada y segura | Autenticación - Firma electrónica | ETSI TS 102 176-1 | ETSI TS 102 176-1. Electronic Signatures and Infrastructures (ESI); Algorithms and parameters for secure electronic signature. Part 1: Hash functions and asymmetric algorithms | Abierto | | 2.0.0 | – | Admitido |
| Accesibilidad multicanal, integrada y segura. | Autenticación - Firma electrónica | PAdES | ETSI TS 102 778-3 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles. | Abierto | | PAdES-1 1.1.1 PAdES-3 1.1.2 PAdES-4 1.1.2 | .p7s .pdf | Admitido |
| Accesibilidad multicanal, integrada y segura | Autenticación - Firma electrónica | PDF Signature | PDF Signature | | Uso generalizado | – | .pdf | En abandono |
| Accesibilidad multicanal, integrada y segura | Autenticación - Firma electrónica | PKCS#7 | PKCS #7: Cryptographic Message Syntax. Version 1.5 | Abierto | | RFC 2315 | – | En abandono |
| Accesibilidad multicanal, integrada y segura | Autenticación - Firma electrónica | (XAdES) | ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES) | Abierto | | 1.2.2 | .xml. .dsig .xsig | Admitido |
| Accesibilidad multicanal, integrada y segura | Autenticación - Firma electrónica | XML-DSig | XML Signature Syntax and Processing. | Abierto | | Second edition. 2008 | .xmp .dsig .xsig .sig | Admitido |
| Accesibilidad multicanal, integrada y segura | Autenticación - Política Firma electrónica | ETSI TR 102 038 | ETS TR 102 038 TC Security - Electronic Signatures and Infrastructures (ESI);XML format for signature policies | Abierto | | RFC 3125 1.1.1 | – | Admitido |
| Accesibilidad multicanal, integrada y segura | Autenticación - Política Firma electrónica | ETS TR 102 272 | ETSI TR 102 272 Electronic Signatures and Infrastructures (ESO; ASN.1 format for signature policies | Abierto | | 1.1.1 | – | Admitido |
| Accesibilidad multicanal, integrada y segura | Cifrado | TLS | Transport Layer Security (TLS) | Abierto | | RFC 5878 RFC 5746 RFC 5705 RFC 5489 RFC 5487 RFC 5469 RFC 5289 RFC 5288 | – | Admitido |
| Accesibilidad multicanal, integrada y segura | Codificación-Codificación de caracteres | Base16, Base32 y Base64 | The Base16, Base32, and Base64 Data Encodings | Abierto | | RFC 4648 | – | Admitido |
| Accesibilidad multicanal, integrada y segura. | Codificación - Codificación de caracteres | UCS UTF | ISO/IEC 10646:2003 Information technology - Universal Multiple-Octet Coded Character Set (UCS) | Abierto | | 2003 | – | Admitido |
| Accesibilidad multicanal, integrada y segura. | Codificación idioma | RFC 4646 ISO 639 | Tags for Identifying Languages. ISO 639 Codes for the representation of names of languages | Abierto | | 2002-2008 RFC 4646 | – | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros - Cartografía vectorial y Sistemas de Información Geográfica | GML | IS0 19136:2007 Geographic information - Geography Markup Language (GML) | Abierto | | 2007 | .gml | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros - Cartografía vectorial y Sistemas de Información Geográfica | WFS | IS0 19142:2010 Geographic information Web Feature Service | Abierto | | 2010 | .gml | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros - Cartografía vectorial y Sistemas de Información Geográfica | WMS | IS0 19128:2005 Geographic information - Web map server interface | Abierto | | 2010 | .gml | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros - Compresión de ficheros | GZIP | GNU Zip | Abierto | | RFC 1952 | .gz | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros - Compresión de ficheros | ZIP | ZIP RFC 1952 | Abierto | | – | .zip | Admitido |

| Cadena de Interoperabilidad | Categoría | Nombre | | Tipo | | Versión (mínima aceptada) | Extensión | Estado |
|---|---|---|---|---|---|---|---|---|
| | | Común | Formal | | | | | |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros - Contenedores multimedia | AVI | Audio Video Interleave | | Uso generalizado | – | .avi | En abandono |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros - Contenedores multimedia | MPEG-4 MP4 media | ISO/IEC 14496-14:2003 Information technology - Coding of audio-visual objects - Part 14: MP4 file format | Abierto | | 2003 | mpeg .mp4 | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | Comma Separated Values. | Comma Separated Values. | Abierto | | RFC 4180 | .csv .txt | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | HTML | HyperText Markup Language | Abierto | | 4.01 | .html .htm | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | CSS | Cascading Style Sheets | Abierto | | 2.1 | .css | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | JPEG | ISO/IEC 15444. Information technology - JPEG 2000 image coding system. | Abierto | | 2004-2008 | .jpg .jpeg | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | MHTML | Multipurpose Internet Mail Extension HTML | Abierto | | RFC 2557 | .mhtml .mht | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | ISO/IEC 263002006 OASIS 1.2 | ISO/IEC 26300:2006 Information technology - Open Document Format for Office Applications (OpenDocument) OASIS 1.2 | Abierto | | 1.0 | .odt .ods .odp .odg | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | Strict Open XML | ISO/IEC 29500-1:2012 Information technology — Document description and processing languages — Office Open XML File Formats — Part 1: Fundamentals and Markup Language Reference - Strict | Abierto | | 2012 | .docx .xlsx .pptx | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | PDF | ISO 32000-1:2008 Document management -Portable document format - Part 1: PDF 1.7 | | Abierto | 1.4 | .pdf | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | PDFA | ISO 19005-1:2005 ISO 19005-2:2011 Document management -Electronic document file format for long-term preservation | Abierto | | 1.4 1.7 | .pdf | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | PMG | ISO/IEC 15948:2004 Information technology - Computer graphics and image processing - Portable Network Graphics (PNG): Functional specification. | Abierto | | 2004 | .png | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | RTF | Rich Text Format. | | Uso generalizado | 1.6 | .rff | En abandono |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | Imagen y/o texto | SVG | Scalable Vector Graphics. | Abierto | 1.1 | .svg | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | TIFF | ISO 12639:2004 Graphic technology - Prepress digital data exchange - Tag image file format for image technology (TIFF/IT) | Abierto | | 2004 | .tiff | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Imagen y/o texto | TXT | Texto plano | Abierto | | – | .txt | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Sonido | MP3. MPEG-1 Audio Layer 3 | ISO/IEC 11172-1:1993 ISO/IEC 11172-2:1993 ISO/IEC 11172-3:1993 ISO/IEC 11172-4:1995 ISO/IEC TR 11172-5:1998 | | Uso generalizado | 1993-1998 | .mp3 | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Sonido | OGG-Vorbis | OGG Vorbis | Abierto | | 2010 | .ogg .oga | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Vídeo | MPEG-4 MP4 Video | ISO/IEC 14496-14:2003 Information technology - Coding of audio-visual objects - Part 14: MP4 file format | | Uso generalizado | 2003 | .mpeg .mp4 | Admitido |
| Accesibilidad multicanal, integrada y segura. | Formatos ficheros-Vídeo | BebM | WebM | Abierto | | 2010 | .webm | Admitido |
| Accesibilidad multicanal, integrada y segura. | Gestión documental y archivística | ISAAR CPF | International Standard Archival Autorithy Records for Corporate Bodies, Persons and Families. | | Uso generalizado | – | – | Admitido |
| Accesibilidad multicanal, integrada y segura. | Gestión documental y archivística | ISAD (G) | General International Standard Archival Description. | | Uso generalizado | – | – | Admitido |
| Accesibilidad multicanal, integrada y segura. | Gestión documental y archivística | ISDF | Norma internacional para la descripción de funciones. | | Uso generalizado | – | – | Admitido |

| Cadena de Interoperabilidad | Categoría | Nombre | | Tipo | | Versión (mínima aceptada) | Extensión | Estado |
|---|---|---|---|---|---|---|---|---|
| | | Común | Formal | | | | | |
| Accesibilidad multicanal, integrada y segura. | Gestión documental y archivística | NEDA | Modelo conceptual de descripción archivística y requisitos de datos básicos de las descripciones de documentos de archivo, agentes y funciones — Parte 1: Tipos de entidad. | | Uso generalizado | 2007 | – | Admitido |
| Accesibilidad multicanal, integrada y segura. | Gestión documental y archivística | UNE-ISO 30300 | UNE-ISO 30300:2011 Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario | Abierto | | 2011 | – | Admitido |
| Accesibilidad multicanal, integrada y segura. | Gestión documental y archivística | UNE-ISO 30301 | UNE-ISO 30301:2011 Información y documentación. Sistemas de gestión para los documentos. Requisitos. | Abierto | | 2011 | – | Admitido |
| Accesibilidad multicanal, integrada y segura. | Gestión documental y archivística | UNE-ISO 15489 | UNE-ISO 15489-1:2006 Parte 1: Generalidades UNE-ISOfTR 15489-2:2006. Parte 2: Directrices. (ISO/TR 15489-2:2001) | Abierto | | 2006 | – | Admitido |
| Accesibilidad multicanal, integrada y segura. | Gestión documental y archivística | UNE-ISO 23081 | UNE-ISO 23081-1:2008 Parte 1: Principios. UNE-ISOfTS 23081-2:2008 Parte 2: Elementos de implementación y conceptuales. | Abierto | | 2008 | – | Admitido |
| Accesibilidad multicanal, integrada y segura. | Integridad | SHA | SHA | Secure Hash Algorithms | Abierto | RFC 4634 RFC 3874 | – | |
| Infraestructuras y servicios asociados | Integridad | LDAP | Lightweight Directory Access Protocol. | Abierto | | RFC 4510 | – | Admitido |
| Infraestructuras y servicios asociados | Protocolos de comunicación e intercambio - Correo electrónico | MIME | Multipurpose Internet Mail Extensions | Abierto | | RFC 2045 | – | Admitido |
| Infraestructuras y servicios asociados | Protocolos de comunicación e intercambio - Correo electrónico | SMTP | Simple Mail Transfer Protocol | Abierto | | RFC 5321 | – | Admitido |
| Infraestructuras y servicios asociados | Protocolos de comunicación e intercambio - Tecnologías de transporte y red | DNS | Domain Name System | Abierto | | RFC 1035 | – | Admitido |
| Infraestructuras y servicios asociados | Protocolos de comunicación e intercambio - Tecnologías de transporte y red | HTTP | Hypertext Transfer Protocol | Abierto | | 1.1 RFC 2616 RFC 2817 | http:// | Admitido |
| Infraestructuras y servicios asociados | Protocolos de comunicación e intercambio - Tecnologías de transporte y red | IPSec | Security Architecture for the Internet Protocol | Abierto | | RFC 2401 RFC 4302 RFC 4835 | – | Admitido |
| Infraestructuras y servicios asociados | Protocolos de comunicación e intercambio - Tecnologías de transporte y red | NTP | Network Time Protocol | Abierto | | RFC 5905 | – | Admitido |
| Integración de sistemas y servicios | Autenticación - Certificados | OCSP | X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP | Abierto | | RFC 2560 | – | Admitido |
| Integración de sistemas y servicios | Autenticación - Sellado de tiempo | ETSI TS 102 023 | ETSI TS 102 023 Electronic Signatures and Infrastructures (ESO; Policy requirements for time-stamping authorities | Abierto | | RFC 3628 | – | Admitido |
| Integración de sistemas y servicios | Protocolos de comunicación e intercambio - Servicios Web | SOAP | Simple Object Access Protocol | Abierto | | 1.1 | – | Admitido |
| Integración de sistemas y servicios | Protocolos de comunicación e intercambio - Servicios Web | UDDI | Universal Discovery, Description and Integration | Abierto | | 3.0 | – | Admitido |
| Integración de sistemas y servicios | Protocolos de comunicación e intercambio - Servicios Web | WSDL | Web Services Definition Language | Abierto | | 1.1 | – | Admitido |
| Integración de sistemas y servicios | Protocolos de comunicación e intercambio - Servicios Web | WS-Security | Web Services Security: SOAP Message Security | Abierto | | 1.1 | – | Admitido |
| Integración de sistemas y servicios | Tecnologías para identificación | ASN.1 | ISOIIEC 8824 Information technology - Abstract Syntax Notation One (ASN.1) | Abierto | | 2008 | – | Admitido |

| Cadena de Interoperabilidad | Categoría | Nombre | | Tipo | | Versión (mínima aceptada) | Extensión | Estado |
|---|---|---|---|---|---|---|---|---|
| | | Común | Formal | | | | | |
| Integración de sistemas y servicios | Tecnologías para identificación | OID | ISO/FDIS 26324 Information and documentation - Digital object identifier system | Abierto | | 2010 | – | Admitido |
| Integración de sistemas y servicios | Tecnologías para identificación | URI | Uniform Resource Identifier | Abierto | | RFC 3986 RFC 5785 | – | Admitido |
| Integración de sistemas y servicios | Tecnologías para identificación | URL | Uniform Resource Locators | Abierto | | RFC 1738 | – | Admitido |
| Integración de sistemas y servicios | Tecnologías para identificación | URN | Uniform Resource Names (URN) Namespaces | Abierto | | – | – | Admitido |
| Modelos e integración de datos. | Métricas | Fechas y horas | ISO 8601:2004 Data elements and interchange formats - Information interchange - Representation of dates and times | Abierto | | 2004 | – | Admitido |
| Modelos e integración de datos. | Protocolos de comunicación e intercambio - Específicos a nivel de aplicación | CODICE | Componentes y Documentos Interoperables para la Contratación Electrónica | Abierto | | 2.0 | .xml | Admitido |
| Modelos e integración de datos. | Protocolos de comunicación e intercambio - Específicos a nivel de aplicación | Facturae | Factura electrónica | Abierto | | 3.0 | .xml | Admitido |
| Modelos e integración de datos. | Protocolos de comunicación e intercambio - Específicos a nivel de aplicación | SCSP | Sustitución de Certificados en papel | Abierto | | 2.0 | – | Admitido |
| Modelos e integración de datos. | Protocolos de comunicación e intercambio - Específicos a nivel de aplicación | SICRES | Sistemas de Información Común de Registros de Entrada y SALIDA (SICRES) | Abierto | | 2.0 3.0 | | Admitido |
| Modelos e integración de datos. | Semántica | DCAT | Data Catalog Vocabulary | Abierto | | – | – | Admitido |
| Modelos e integración de datos. | Semántica - Metadatos | MoReq | Model Requirements for the management of electronic records. | Abierto | | – | – | Admitido |
| Modelos e integración de datos. | Semántica - Metadatos | PREMIS | PREservation Metadata: Implementation Strategies. V2.1 | | Uso generalizado | – | – | Admitido |
| Modelos e integración de datos. | Semántica - Metadatos | INSPIRE Metadata Regulation | Commission Regulation (EC) No 1205/2008 of 3 December 2008 implementing Directive 2007/2/EC of the European Parliament and of the Council as regards metadata (Text with EEA relevance) | Abierto | | – | | Admitido |
| Modelos e integración de datos. | Semántica - Tecnologías semánticas | N3 | Notation3 | Abierto | | – | .n3 | Admitido |
| Modelos e integración de datos. | Semántica - Tecnologías semánticas | OWL | Ontology Web Language | Abierto | | 2.0 | – | Admitido |
| Modelos e integración de datos. | Semántica - Tecnologías semánticas | RDF | Resource Description Framework | Abierto | | 1.0 | – | Admitido |
| Modelos e integración de datos. | Semántica - Tecnologías semánticas | RDFa | Resource Description Framework –in– attributes | Abierto | | 2008 | – | Admitido |
| Modelos e integración de datos. | Semántica - Tecnologías semánticas | SKOS | Simple Knowledge Organization System | Abierto | | 2009 | – | Admitido |
| Modelos e integración de datos. | Semántica - Tecnologías semánticas | SPARQL | Query Language for RDF | Abierto | | 2008 | – | Admitido |
| Modelos e integración de datos. | Semántica - Tecnologías semánticas | Turtle | Terse RDF Triple Language | Abierto | | 2011 | .ttl | Admitido |
| Modelos e integración de datos. | Tecnologías de integración de datos | XML | Extensible Markup Language (XML) | Abierto | | 1.0 | .xml | Admitido |
| Modelos e integración de datos. | Tecnologías de integración de datos | XSD | XML Schema | Abierto | | 1.0 | .xsd | Admitido |

# § 14

## Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico

Ministerio de Política Territorial y Administración Pública
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13169

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

En particular, la Norma Técnica de Interoperabilidad de Documento electrónico establece los componentes del documento electrónico, incluyendo contenido, firma electrónica y

metadatos mínimos obligatorios, y su formato, así como las condiciones para su intercambio y reproducción; para los aspectos relativos a la gestión y conservación de los documentos electrónicos se remite a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos; finalmente, se incluye en anexo la definición detallada de los metadatos mínimos obligatorios, los esquemas XML para intercambio de documentos y la información básica de firma de documentos electrónicos. En este sentido, la estructura de documento electrónico definida en esta norma permite la utilización de las firmas electrónicas contempladas en la Decisión de la Comisión 2011/130/EU de 25 de febrero de 2011 por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Documento electrónico, cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Documento electrónico que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la Disposición Transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

## NORMA TÉCNICA DE INTEROPERABILIDAD DE DOCUMENTO ELECTRÓNICO

*I. Objeto.*

La Norma Técnica de Interoperabilidad de Documento electrónico tiene por objeto establecer los componentes del documento electrónico, contenido, en su caso, firma electrónica y metadatos, así como la estructura y formato para su intercambio.

*II. Ámbito de aplicación.*

Esta norma será de aplicación en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica a:

a) Documentos administrativos electrónicos.

b) Cualquier otro documento electrónico susceptible de formar parte de un expediente electrónico.

*III. Componentes del documento electrónico.*

Los componentes de un documento electrónico son:

a) Contenido, entendido como conjunto de datos o información del documento.

b) En su caso, firma electrónica.

c) Metadatos del documento electrónico.

*IV. Firma del documento electrónico.*

Los documentos administrativos electrónicos, y aquellos susceptibles de formar parte de un expediente, tendrán siempre asociada al menos una firma electrónica de acuerdo con la normativa aplicable.

*V. Metadatos del documento electrónico.*

V.1 Los metadatos mínimos obligatorios del documento electrónico:

a) Serán los definidos en el anexo I.

b) Estarán presentes en cualquier proceso de intercambio de documentos electrónicos entre órganos de la Administración y Entidades de Derecho Público vinculadas o dependientes de aquélla y con el ciudadano.

c) No serán modificados en ninguna fase posterior del procedimiento administrativo, a excepción de modificaciones necesarias para la corrección de errores u omisiones en el valor inicialmente asignado.

V.2 Se podrán asignar metadatos complementarios para atender a necesidades de descripción específicas.

Estos metadatos complementarios se aplicarán, en su caso, de acuerdo con lo previsto en la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

V.3 Cada órgano de la Administración y Entidad de Derecho Público vinculada o dependiente de aquélla implementará en su propio ámbito de actuación los metadatos de los documentos electrónicos para su tratamiento y gestión a nivel interno. Además, garantizará la disponibilidad e integridad de los metadatos de sus documentos electrónicos, manteniendo de manera permanente las relaciones entre el documento y sus metadatos.

*VI. Formato de documentos electrónicos.*

VI.1 Los ficheros de contenido de los documentos electrónicos se ajustarán a los formatos establecidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares.

VI.2 La elección del formato se realizará conforme a la naturaleza de la información a tratar primando la finalidad para la cual fue definido cada formato.

VI.3 Se podrán utilizar otros formatos cuando existan particularidades que lo justifiquen o sea necesario para asegurar el valor probatorio del documento electrónico y su fiabilidad como evidencia electrónica de las actividades y procedimientos en caso de proceder a su conversión de formato.

*VII. Intercambio de documentos electrónicos.*

VII.1 Todo documento electrónico objeto de intercambio tendrá los componentes definidos en el apartado III de esta norma.

VII.2 El intercambio de documentos electrónicos se realizará mediante su envío según la estructura definida en el anexo II, sin perjuicio de la aplicación de otras reguladas por su normativa específica.

VII.3 Excepcionalmente, se podrán aplicar otras estructuras para el intercambio de documentos electrónicos entre Administraciones públicas, cuando exista acuerdo previo entre las partes. En cualquier caso, si debe enviarse a un tercero, la estructura utilizada será convertida por el emisor a la estructura definida en el anexo II.

VII.4 Para el intercambio de documentos electrónicos, entre Administraciones públicas, en procesos de actuación automatizada:

a) Se utilizará preferentemente la Red de comunicaciones de las Administraciones públicas españolas como medio para la transmisión.

b) Si el documento electrónico forma parte de un asiento registral, éste será tratado como documento adjunto al mensaje de datos de intercambio según lo establecido en la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales.

VII.5 En caso de intercambio de documentos electrónicos entre Administraciones públicas que suponga una transferencia de custodia o traspaso de responsabilidad de gestión de documentos que deban conservarse permanentemente, el órgano o entidad trasferidora verificará la autenticidad e integridad del documento en el momento de dicho intercambio.

*VIII. Acceso a documentos electrónicos.*

Cuando las administraciones públicas faciliten el acceso a los documentos electrónicos a través de sus sedes electrónicas o de los canales de comunicación que correspondan en cada caso, se mostrará:

a) El contenido del documento electrónico cuando éste sea representable conforme a lo recogido sobre formatos en el apartado VI de esta norma.

b) La información básica de cada una de las firmas del documento definida en el anexo III.

c) Descripción y valor de los metadatos mínimos obligatorios.

## ANEXO I

### Metadatos mínimos obligatorios del documento electrónico

| Metadato | Descripción/Condiciones de uso | ¿Repetible?[1] | Tipo | Esquema de valores |
|---|---|---|---|---|
| Versión N11 | Identificador normalizado de la versión de la Norma Técnica de Interoperabilidad de Documento electrónico conforme a la cual se estructura el documento electrónico. | 1 | URI | http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e |
| Identificador | Identificador normalizado del documento. | 1 | Cadena de caracteres | ES_ <Órgano>_<AAAA>_<ID específico>[2]<br>Ejemplo: ES E00010207 2010 MPR0000000000000000000000010207 |
| Órgano | Identificador normalizado de la administración generadora del documento o que realiza la captura del mismo. | 1:N | Cadena de caracteres | Código alfanumérico único para cada órgano/unidad/oficina extraído del Directorio Común gestionado por el Ministerio de Política Territorial y Administración Pública. |
| Fecha de captura | Fecha de alta del documento en el sistema de gestión documental. | 1 | Fecha/hora | Formato: AAAAMMDD T HH:MM:SS <ISO 8601> |
| Origen | Indica si el contenido del documento fue creado por un ciudadano o por una administración. | 1 | Lógico | '0' = Ciudadano '1' = Administración |
| Estado de elaboración | Indica la naturaleza del documento. Si es copia, este metadato indica también si se ha realizado una digitalización o conversión de formato en el proceso de generación. | 1 | Cadena de caracteres | – Original (Ley 11/2007 Ad. 30).<br>– Copia electrónica auténtica con cambio de formato (Ley 11/2007Art.30.1).<br>– Copia electrónica auténtica de documento papel (Ley 11/2007 Art.30.2 y 30.3).<br>– Copia electrónica parcial auténtica. Otros. |
| Nombre de formato | Formato lógico del fichero de contenido del documento electrónico. | 1 | Cadena de caracteres | Valor extraído de la lista de formatos admitidos para ficheros definidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares. |
| | | | | Documentos de decisión: |
| | | | | – Resolución. |
| | | | | – Acuerdo. |
| | | | | – Contrato. |
| | | | | – Convenio. |
| | | | | – Declaración. |
| | | | | Documentos de transmisión: |
| | | | | – Comunicación. |
| | | | | – Notificación. |
| | | | | – Publicación. |
| | | | | – Acuse de recibo. |
| Tipo documental | Descripción del tipo documental del documento. | 1 | Cadena de caracteres | Documentos de constancia: |
| | | | | – Acta. |
| | | | | – Certificado. |
| | | | | – Diligencia. |
| | | | | Documentos de juicio: |
| | | | | – Informe. |
| | | | | Documentos de ciudadano: |
| | | | | – Solicitud. |
| | | | | – Denuncia. |
| | | | | – Alegación. |
| | | | | – Recursos. |
| | | | | – Comunicación ciudadano. |
| | | | | – Factura. |
| | | | | – Otros incautados. |
| | | | | Otros. |

| Metadato | Descripción/Condiciones de uso | ¿Repetible?[1] | Tipo | Esquema de valores |
|---|---|---|---|---|
| Tipo de firma | Indica el tipo de firma que avala el documento. En caso de firma con certificado, indica el formato de la firma. | 1:N | Cadena de caracteres | – CSV<br>– Formatos de firma electrónica de documentos electrónicos definidos en la Norma Técnica de Interoperabilidad de Política de firma y certificados de la Administración. |
| Si «Tipo de firma» = CSV | | | | |
| Valor CSV | Valor del CSV. | 1:N | Cadena de caracteres | NIA |
| Definición generación CSV | Referencia a la Orden, Resolución o documento que define la creación del CSV correspondiente. | 1:N | Cadena de caracteres | Si AGE:<br>Referencia BOE:BOE A YYYY-XXXXX<br>En otro caso, referencia correspondiente. |
| Si «Estado de elaboración» = | | | | |
| – Copia electrónica auténtica con cambio de formato (Ley 11/2007Art.30.1). | | | | |
| – Copia electrónica parcial auténtica. | | | | |
| Identificador de documento origen | Identificador normalizado del documento origen al que corresponde la copia. | 1 | Cadena de caracteres | Si el documento origen es un documento electrónico:<br>ES_<Órgano>_<AAAA>_<ID específico><br>Ejemplo: ES–E00010207–2010 MPR00000000000000000000000010207 |

[1] Nótese que la repetibilidad indicada en la tabla sólo se refiere a los metadatos que acompañan al documento electrónico en un intercambio, sin perjuicio de la posibilidad de asignación de otros metadatos gestionados a nivel interno de cada administración cuyas consideraciones atenderán a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

[2] Codificación del Identificador del documento:

<Órgano>: Véase codificación del metadato «Órgano». En caso de más un órgano los nueve caracteres correspondientes serán acordados entre las partes con el fin de asegurarla unicidad del identificador que es su único fin.

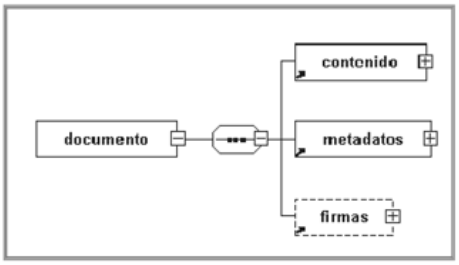
<AAAA>: Año de la fecha de captura del documento. (Longitud: 4 caracteres).

<ID específico>: Código alfanumérico que identifica de forma única al documento dentro de los generados por la administración responsable. Cada administración puede diseñar el proceso de generación según sus necesidades, asegurando en cualquier caso su unicidad. Por lo tanto, este ID puede generarse de forma secuencia) o bien, ser una réplica del ID utilizado a nivel interno de la administración. (Longitud: 30 caracteres).

## ANEXO II

## Esquemas XML para intercambio de documentos electrónicos

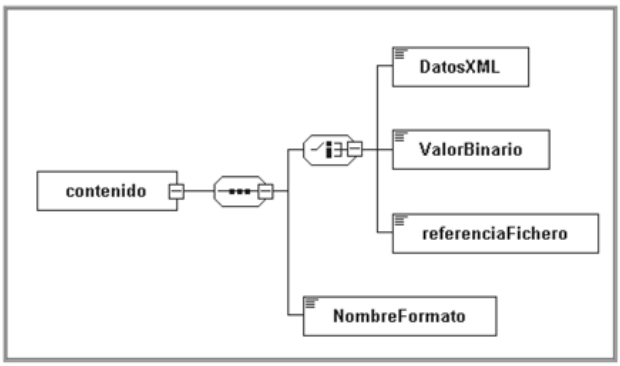
1. *XSD Documento electrónico*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma"
xmlns:enidocmeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/metadatos"
xmlns:enifile="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
xmlns:enidoc="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e"
elementFormDefault="qualified" attributeFormDefault="unqualified">
    <xsd:annotation>
        <xsd:documentation xml:lang="es">XSD DOCUMENTO ENI (v1.0)</xsd:documentation>
    </xsd:annotation>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/metadatos" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-
e/metadatos/metadatosDocumentoEni.xsd"/>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma/firmasEni.xsd"/>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-
e/contenido/contenidoDocumentoEni.xsd"/>
<xsd:element name="documento" type="enidoc:TipoDocumento">
    <xsd:annotation>
<xsd:documentation xml:lang="es">El elemento "documento" podrá aparecer como elemento raíz de un documento XML objeto de intercambio o como elemento no raíz (elemento hijo).</xsd:documentation>
    </xsd:annotation>
</xsd:element>
<xsd:complexType name="TipoDocumento">
    <xsd:sequence>
        <xsd:element ref="enifile:contenido"/>
        <xsd:element ref="enidocmeta:metadatos"/>
        <xsd:element ref="enids:firmas" minOccurs="0" maxOccurs="1">
            <xsd:annotation>
<xsd:documentation xml:lang="es">La firma es obligatoria para el documento administrativo electrónico y para todo aquel documento electrónico susceptible de ser incorporado en un expediente
electrónico.</xsd:documentation>
            </xsd:annotation>
```

```
        </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

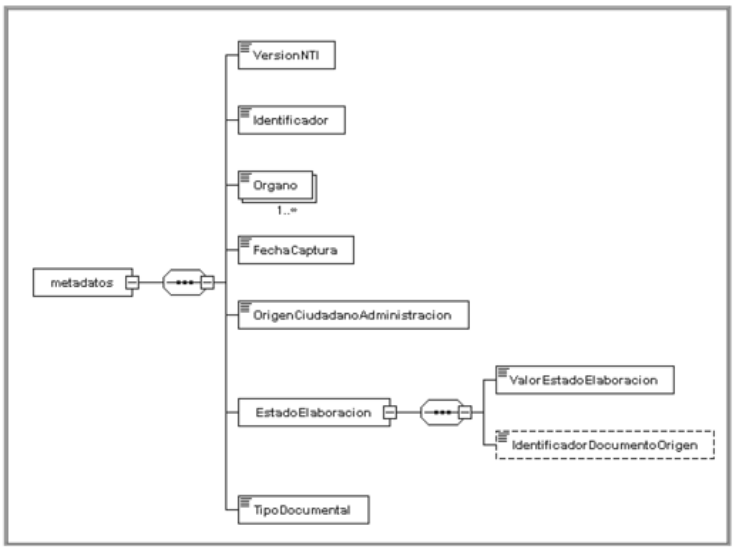
2. *XSD Contenido*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:enifile="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
    <xsd:documentation xml:lang="es">XSD CONTENIDO DOCUMENTO ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:element name="contenido" type="enifile:TipoContenido"/>
<xsd:complexType name="TipoContenido">
    <xsd:sequence>
        <xsd:choice>
            <xsd:element name="DatosXML" type="xsd:anyType">
                <xsd:annotation>
<xsd:documentation xml:lang="es">Contenido en formato XML. En caso de datos XML cuya codificación difiera de la de esta estructura raíz se incluirá una cláusula CDATA.</xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:element name="ValorBinario" type="xsd:base64Binary">
                <xsd:annotation>
                    <xsd:documentation xml:lang="es">Contenido en base64.</xsd:documentation>
                </xsd:annotation>
            </xsd:element>
```

```
            <xsd:element name="referenciaFichero" type="xsd:string">
                <xsd:annotation>
<xsd:documentation xml:lang="es">Referencia interna al fichero de contenido. </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
        </xsd:choice>
        <xsd:element name="NombreFormato" type="xsd:string">
            <xsd:annotation>
                <xsd:documentation xml:lang="es">El formato del fichero de contenido del documento electrónico atenderá a lo establecido en la NTI de Catálogo de estándares.</xsd:documentation>
            </xsd:annotation>
        </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

3. *XSD Metadatos*

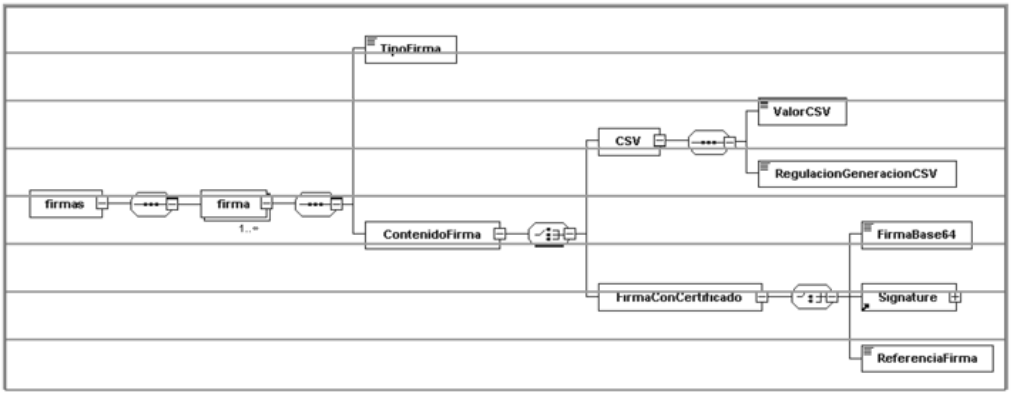


```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:enidocmeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/metadatos"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/metadatos"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
    <xsd:documentation xml:lang="es">XSD METADATOS DOCUMENTO ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:element name="metadatos" type="enidocmeta:TipoMetadatos"/>
<xsd:complexType name="TipoMetadatos">
    <xsd:sequence>
        <xsd:element name="VersionNTI" type="xsd:anyURI"/>
        <xsd:element name="Identificador" type="xsd:string"/>
        <xsd:element name="Organo" type="xsd:string" minOccurs="1" maxOccurs="unbounded"/>
        <xsd:element name="FechaCaptura" type="xsd:dateTime"/>
        <xsd:element name="OrigenCiudadanoAdministracion" type="xsd:boolean"/>
        <xsd:element name="EstadoElaboracion" type="enidocmeta:TipoEstadoElaboracion">
            <xsd:annotation>
                <xsd:documentation xml:lang="es">
- EE01 - Original.
- EE02 - Copia electrónica auténtica con cambio de formato.
- EE03 - Copia electrónica auténtica de documento papel.
- EE04 - Copia electrónica parcial auténtica.
- EE99 - Otros.
                </xsd:documentation>
            </xsd:annotation>
        </xsd:element>
        <xsd:element name="TipoDocumental" type="enidocmeta:tipoDocumental">
            <xsd:annotation>
                <xsd:documentation xml:lang="es">/*Documentos de decisión*/
- TD01 - Resolución.
- TD02 - Acuerdo.
- TD03 - Contrato.
- TD04 - Convenio.
- TD05 - Declaración.
/*Documentos de transmisión*/
- TD06 - Comunicación.
- TD07 - Notificación.
- TD08 - Publicación.
- TD09 - Acuse de recibo.
/*Documentos de constancia*/
- TD10 - Acta.
- TD11 - Certificado.
- TD12 - Diligencia.
/*Documentos de juicio*/
- TD13 - Informe.
/*Documentos de ciudadano*/
- TD14 - Solicitud.
- TD15 - Denuncia.
- TD16 - Alegación.
```

```
- TD17 - Recursos.
- TD18 - Comunicación ciudadano.
- TD19 - Factura.
- TD20 - Otros incautados.
/*Otros*/
- TD99 - Otros.
</xsd:documentation>
                </xsd:annotation>
            </xsd:element>
        </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
<xsd:complexType name="TipoEstadoElaboracion">
        <xsd:sequence>
            <xsd:element name="ValorEstadoElaboracion" type="enidocmeta:enumeracionEstadoElaboracion"/>
            <xsd:element name="IdentificadorDocumentoOrigen" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        </xsd:sequence>
</xsd:complexType>

<!-- Enumeración de estados de elaboración -->
<xsd:simpleType name="enumeracionEstadoElaboracion">
        <xsd:restriction base="xsd:string">
            <xsd:enumeration value="EE01"/>
            <xsd:enumeration value="EE02"/>
            <xsd:enumeration value="EE03"/>
            <xsd:enumeration value="EE04"/>
            <xsd:enumeration value="EE99"/>
        </xsd:restriction>
</xsd:simpleType>

<!-- Enumeración de tipos documentales -->
<xsd:simpleType name="tipoDocumental">
        <xsd:restriction base="xsd:string">
            <xsd:enumeration value="TD01"/>
            <xsd:enumeration value="TD02"/>
            <xsd:enumeration value="TD03"/>
            <xsd:enumeration value="TD04"/>
            <xsd:enumeration value="TD05"/>
            <xsd:enumeration value="TD06"/>
            <xsd:enumeration value="TD07"/>
            <xsd:enumeration value="TD08"/>
            <xsd:enumeration value="TD09"/>
            <xsd:enumeration value="TD10"/>
            <xsd:enumeration value="TD11"/>
            <xsd:enumeration value="TD12"/>
            <xsd:enumeration value="TD13"/>
            <xsd:enumeration value="TD14"/>
            <xsd:enumeration value="TD15"/>
            <xsd:enumeration value="TD16"/>
```

```
            <xsd:enumeration value="TD17"/>
            <xsd:enumeration value="TD18"/>
            <xsd:enumeration value="TD19"/>
            <xsd:enumeration value="TD20"/>
            <xsd:enumeration value="TD99"/>
        </xsd:restriction>
</xsd:simpleType>
</xsd:schema>
```

4. *XSD Firmas*




```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma "
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma " elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
    <xsd:documentation xml:lang="es">XSD FIRMAS ELECTRONICAS ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
<xsd:element name="firmas" type="enids:firmas"/>
<xsd:complexType name="firmas">
    <xsd:sequence>
        <xsd:element name="firma" type="enids:TipoFirmasElectronicas" minOccurs="1" maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="TipoFirmasElectronicas">
    <xsd:sequence>
        <xsd:element name="TipoFirma">
            <xsd:annotation>
                <xsd:documentation xml:lang="es">
```

```
                - TF01 - CSV.
                - TF02 - XAdES internally detached signature.
                - TF03 - XAdES enveloped signature.
                - TF04 - CAdES detached/explicit signature.
                - TF05 - CAdES attached/implicit signature.
                - TF06 - PAdES.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:simpleType>
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="TF01"/>
                <xsd:enumeration value="TF02"/>
                <xsd:enumeration value="TF03"/>
                <xsd:enumeration value="TF04"/>
                <xsd:enumeration value="TF05"/>
                <xsd:enumeration value="TF06"/>
            </xsd:restriction>
        </xsd:simpleType>
    </xsd:element>
    <xsd:element name="ContenidoFirma">
        <xsd:complexType>
            <xsd:choice>
                <xsd:element name="CSV">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="ValorCSV" type="xsd:string"/>
                            <xsd:element name="RegulacionGeneracionCSV" type="xsd:string"/>
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
                <xsd:element name="FirmaConCertificado">
                    <xsd:complexType>
                        <xsd:choice>
                            <xsd:element name="FirmaBase64" type="xsd:base64Binary"/>
                            <xsd:element ref="ds:Signature"/>
                            <xsd:element name="ReferenciaFirma">
                                <xsd:annotation>
                                <xsd:documentation  xml:lang="es">
                                 Referencia interna al fichero que incluye la firma.</xsd:documentation>
                                </xsd:annotation>
                            </xsd:element>
                        </xsd:choice>
                    </xsd:complexType>
                </xsd:element>
            </xsd:choice>
        </xsd:complexType>
    </xsd:element>
</xsd:sequence>
<xsd:attribute name="Id" type="xsd:ID" use="optional"/>
<xsd:attribute name="ref" type="xsd:string" use="optional">

    <xsd:annotation>
        <xsd:documentation xml:lang="es">Almacena el identificador del nodo que se está firmando. En caso de firmas multinodo, se incluirá una lista separada por comas de los identificadores de los nodos
firmados.</xsd:documentation>
    </xsd:annotation>
</xsd:attribute>
</xsd:complexType>
</xsd:schema>
```

## ANEXO III

## Información básica de la firma de documentos electrónicos

| Tipo de firma | Información | Localización |
|---|---|---|
| CSV | Valor del código seguro de verificación. | Metadato del documento electrónico. |
| Firma basada en certificados | Validez de la firma. | Según reglas de validación de firma descritas en la Norma Técnica de Interoperabilidad de Política de firma y certificados de la Administración. |
| | Información del firmante(s) del documento (persona física, jurídica o sello de órgano). | Propiedades o etiquetas de la firma. |
| | Emisor del certificado del firmante(s). | Propiedades o etiquetas de la firma. |
| | Fecha y hora de la firma(s). | Propiedades o etiquetas de la firma. |

# § 15

## Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Digitalización de Documentos

Ministerio de Política Territorial y Administración Pública
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13168

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

En particular, la Norma Técnica de Interoperabilidad de Digitalización de Documentos establece los componentes de un documento electrónico digitalizado, incluyendo la imagen

electrónica, firma electrónica y metadatos, así como las reglas para la digitalización de documentos en soporte papel por parte de las Administraciones públicas, atendiendo a los formatos, niveles de calidad, condiciones técnicas y estándares aplicables; y para los aspectos relativos a la gestión y conservación de los documentos electrónicos digitalizados se remite a la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la Disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Digitalización de Documentos, cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Digitalización de Documentos que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

## NORMA TÉCNICA DE INTEROPERABILIDAD DE DIGITALIZACIÓN DE DOCUMENTOS

### *I. Objeto*

La Norma Técnica de Interoperabilidad de Digitalización de Documentos tiene por objeto establecer los requisitos a cumplir en la digitalización de documentos en soporte papel o en otro soporte no electrónico susceptible de digitalización a través de medios fotoeléctricos.

### *II. Ámbito de aplicación*

Esta norma será de aplicación en la digitalización de documentos en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

### *III. Documentos electrónicos digitalizados*

III.1 La digitalización de un documento para la generación de un documento electrónico atenderá a lo dispuesto en la Norma Técnica de Interoperabilidad de Documento Electrónico y estará compuesto por:

a) La imagen electrónica que representará el aspecto y contenido del documento en el soporte origen y cumplirá los requisitos establecidos en el apartado IV de esta norma.

b) Los metadatos mínimos obligatorios definidos en la Norma Técnica de Interoperabilidad de Documento Electrónico.

Se podrán asignar metadatos complementarios para atender a necesidades de descripción específicas del proceso de digitalización que se aplicarán, en su caso, de acuerdo con lo previsto en la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos.

c) Si procede, firma de la imagen electrónica de acuerdo con la normativa aplicable.

III.2 Para que el documento electrónico digitalizado sea copia auténtica del documento origen, se cumplirán, adicionalmente, los requisitos establecidos en la Norma Técnica de

Interoperabilidad de Procedimientos de Copiado Auténtico y Conversión entre Documentos Electrónicos.

*IV. Requisitos de la imagen electrónica*

IV.1 Las imágenes electrónicas aplicarán los formatos establecidos para ficheros de imagen en la Norma Técnica de Interoperabilidad de Catálogo de Estándares.

IV.2 El nivel de resolución mínimo para imágenes electrónicas será de 200 píxeles por pulgada, tanto para imágenes obtenidas en blanco y negro, color o escala de grises.

IV.3 La imagen electrónica será fiel al documento origen, para lo cual:

a) Respetará la geometría del documento origen en tamaños y proporciones.
b) No contendrá caracteres o gráficos que no figurasen en el documento origen.
c) Su generación atenderá a lo establecido en el apartado V de esta norma.

*V. Proceso de digitalización*

Con el fin de satisfacer los requisitos establecidos en el apartado IV, la digitalización de un documento:

1. Se realizará a través de un proceso informático en el que, garantizando la integridad de cada uno de los pasos, se realizarán las siguientes tareas:

a) Digitalización por un medio fotoeléctrico, de modo que se obtenga una imagen electrónica en la memoria del sistema asociado al dispositivo.
b) Si procede, optimización automática de la imagen electrónica para garantizar su legibilidad, de modo que todo contenido del documento origen pueda apreciarse y sea válido para su gestión (umbralización, reorientación, eliminación de bordes negros, u otros de naturaleza análoga).
c) Asignación de los metadatos al documento electrónico digitalizado según lo dispuesto en el apartado 111.1.
d) Si procede, firma de la imagen electrónica.

2. Contemplará la aplicación de un conjunto de operaciones de mantenimiento preventivo y comprobaciones rutinarias que permitirán garantizar mediante su cumplimiento que, en todo momento, el estado de la aplicación de digitalización y los dispositivos asociados producirán imágenes fieles al documento en soporte papel.

# § 16

## Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico

Ministerio de Política Territorial y Administración Pública
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13170

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

En particular, la Norma Técnica de Interoperabilidad de Expediente electrónico establece la estructura de los expedientes electrónicos, que incluye documentos electrónicos, índice

electrónico, firma electrónica y metadatos mínimos obligatorios, así como las especificaciones para los servicios de remisión y puesta a disposición; para los aspectos relativos a la gestión y conservación de los expedientes electrónicos se remite a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos; finalmente, se incluye en anexo la definición detallada de los metadatos mínimos obligatorios y los esquemas XML para el intercambio de expedientes electrónicos. En este sentido, la estructura de expediente electrónico definida en esta norma permite la utilización de las firmas electrónicas contempladas en la Decisión de la Comisión 2011/130/EU, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Expediente electrónico, cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Expediente electrónico que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la Disposición Transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

**NORMA TÉCNICA DE INTEROPERABILIDAD DE EXPEDIENTE ELECTRÓNICO**

*I. Objeto.*

La Norma Técnica de Interoperabilidad de Expediente electrónico tiene por objeto establecer la estructura y el formato del expediente electrónico, así como las especificaciones de los servicios de remisión y puesta a disposición.

*II. Ámbito de aplicación.*

II.1 Esta norma será de aplicación a los expedientes electrónicos en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

II.2 Las condiciones establecidas en esta norma se podrán aplicar a otros conjuntos de documentos electrónicos que, habiendo sido creados al margen de un procedimiento reglado, se hubiesen formado mediante agregación, como resultado de una secuencia de actuaciones coherentes que conducen a un resultado específico.

*III. Componentes del expediente electrónico.*

III.1 Los componentes de un expediente electrónico son:

a) Documentos electrónicos, que cumplirán las características de estructura y formato establecidas en la Norma Técnica de Interoperabilidad de Documento electrónico.

Los documentos electrónicos podrán incluirse en un expediente electrónico bien directamente como elementos independientes, bien dentro de una carpeta, entendida ésta como una agrupación de documentos electrónicos creada por un motivo funcional, o bien como parte de otro expediente, anidado en el primero.

b) Índice electrónico, que según lo establecido en el artículo 32.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, garantizará la integridad del expediente electrónico y permitirá su recuperación siempre que sea preciso.

El índice electrónico recogerá el conjunto de documentos electrónicos asociados al expediente en un momento dado y, si es el caso, su disposición en carpetas o expedientes.

c) Firma del índice electrónico por la Administración, órgano o entidad actuante de acuerdo con la normativa aplicable.

d) Metadatos del expediente electrónico.

III.2 La incorporación de un expediente electrónico a un sistema de gestión documental atenderá a lo dispuesto en la Norma Técnica de Interoperabilidad de Documento electrónico y en la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

*IV. Metadatos del expediente electrónico.*

IV.1 Los metadatos mínimos obligatorios del expediente electrónico:

a) Serán los definidos en el anexo I.

b) Se asociarán en la formación del expediente para su remisión o puesta a disposición.

c) No serán modificados en ninguna fase posterior del procedimiento administrativo, a excepción de modificaciones necesarias para la corrección de errores u omisiones en el valor inicialmente asignado.

IV.2 Se podrán asignar metadatos complementarios para atender a necesidades de descripción específicas. Estos metadatos complementarios se aplicarán, en su caso, de acuerdo con lo previsto en la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

*V. Intercambio de expedientes electrónicos.*

V.1 El intercambio de expedientes electrónicos, a los efectos de remisión y puesta a disposición, se realizará mediante el envío en primer lugar de la estructura definida en el anexo II, sin perjuicio de la aplicación de otras, reguladas por su normativa específica. Tras el envío de dicha estructura, se enviarán cada uno de los documentos electrónicos que componen el expediente, en el orden indicado en el índice y atendiendo a lo establecido en la Norma Técnica de Interoperabilidad de Documento electrónico.

V.2 Excepcionalmente, se podrán aplicar otras estructuras para el intercambio de expedientes electrónicos entre Administraciones públicas, cuando exista acuerdo previo entre las partes. En cualquier caso, si debe enviarse a un tercero, la estructura utilizada será convertida por el emisor a la estructura definida en el anexo II.

V.3 Cuando la naturaleza o la extensión de las pruebas o documentos que forman parte del expediente electrónico no permitan o dificulten notablemente su inclusión en una de las estructuras establecidas, se incorporará al expediente electrónico un documento en el que se especifique cuales son estas pruebas o documentos. Dichas pruebas o documentos serán custodiados por el órgano gestor sin perjuicio, en su caso, de aportación separada cuando así se requiera.

V.4 El índice electrónico de los expedientes objeto de intercambio reflejará, al menos:

a) La fecha de generación del índice.

b) Para cada documento electrónico: su identificador, su huella digital, la función resumen utilizada para su obtención, que atenderá a lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares, y, opcionalmente, la fecha de incorporación al expediente y el orden del documento dentro del expediente.

c) Si es el caso, la disposición de los documentos en carpetas y expedientes electrónicos anidados.

V.5 Para el intercambio de expedientes electrónicos, entre Administraciones públicas, en procesos de actuación automatizada:

a) Se utilizará preferentemente la Red de comunicaciones de las Administraciones públicas españolas como medio para la transmisión.

b) Si el expediente electrónico forma parte de un asiento registral, éste será tratado como adjunto del mensaje de datos de intercambio según lo establecido en la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales.

V.6 En caso de intercambio de expedientes electrónicos entre Administraciones públicas que suponga una transferencia de custodia o traspaso de responsabilidad de gestión de expedientes que deban conservarse permanentemente, el órgano o entidad transferidora verificará la autenticidad e integridad del expediente en el momento de dicho intercambio.

## ANEXOS

## ANEXO I

### Metadatos mínimos obligatorios de expedientes electrónicos

| Metadato | Descripción/Condiciones de uso | ¿Repetible?1 F[1] | Tipo | Esquema de valores |
|---|---|---|---|---|
| Versión NTI | Identificador normalizado de la versión de la Norma Técnica de Interoperabilidad de Expediente electrónico conforme a la cual se estructura el expediente. | 1 | URI | http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e |
| Identificador | Identificador normalizado del expediente. | 1 | Cadena de caracteres | ES <órganoUU><AAAA> EXP <ID especifico>2F[2]<br>Ejemplo: ES_E00010207_2010_EXP_ MPR000000000000000000000010207 |
| Órgano | Identificador normalizado de la administración responsable de la tramitación del procedimiento | 1:N | Cadena de caracteres | Código alfanumérico único para cada órgano/unidad/oficina extraído del Directorio Común gestionado por el Ministerio de Política Territorial y Administración Pública.<br>UEjemploU: E00003901 |
| Fecha Apertura Expediente | Fecha de apertura del expediente | 1 | Fecha/hora | Formato: AAAAMMDD T HH:MM:SS<br><ISO 8601> |
| Clasificación | Procedimiento administrativo con el que se relaciona el expediente | 1 | Cadena de caracteres | Esquema de valores normalizado según el Sistema de Información Administrativa (SIA).<br>Si el procedimiento no se encuentra en SIA:<br><órgano >_PRO_<ID_PRO_especifico>3F[3] |
| Estado | Estado del expediente en el momento de intercambio. | 1 | Cadena de caracteres | – Abierto<br>– Cerrado<br>– Índice para remisión cerrado. |
| Interesado | Identificador del interesado. | 0:N | Cadena de caracteres | a) Si ciudadano o persona jurídica: DNI, NIE, NIF o similar.<br>b) Si administración: <ÓrganoUU> |
| Tipo de firma | Indica el tipo de firma del índice del expediente | 1:N | Cadena de caracteres | – CSV'<br>– Formatos de firma electrónica de documentos electrónicos definidos en la Norma Técnica de Interoperabilidad de Política de firma y certificados de la Administración. |
| Si "Tipo de firma" = CSV | | | | |
| Valor CSV | Valor del CSV. | 1:N | Cadena de caracteres | N/A |
| Definición generación CSV | Referencia a la Orden, Resolución o documento que define la creación del CSV correspondiente. | 1:N | Cadena de caracteres | Si AGE:<br>Referencia BOE:BOE-A-YYYY-XXXXX<br>En otro caso, referencia correspondiente. |

[1] Nótese que la repetibilidad indicada en la tabla sólo se refiere a los metadatos que acompañan al expediente electrónico en un intercambio, sin perjuicio de la posibilidad de asignación de otros metadatos gestionados a nivel interno de cada administración cuyas consideraciones atenderán a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

[2] Codificación del Identificador del expediente:

<Órgano>: Véase codificación del metadato "Órgano". En caso de más de un órgano los nueve caracteres correspondientes serán acordados entre las partes con el fin de asegurar la unicidad del identificador que es su único fin.

<AAAA>: Año de la fecha de creación del expediente. (Longitud: 4 caracteres).

<ID_específico>: Código alfanumérico que identifica de forma única al expediente dentro de los generados por la administración responsable. Cada administración puede diseñar el proceso de generación según sus necesidades, asegurando en cualquier caso su unicidad. Por lo tanto, este ID puede generarse de forma secuencial o bien, ser una réplica del ID utilizado a nivel interno de la administración. (Longitud: 30 caracteres).

[3] Codificación del metadato Calificación si el procedimiento no existe en SIA:

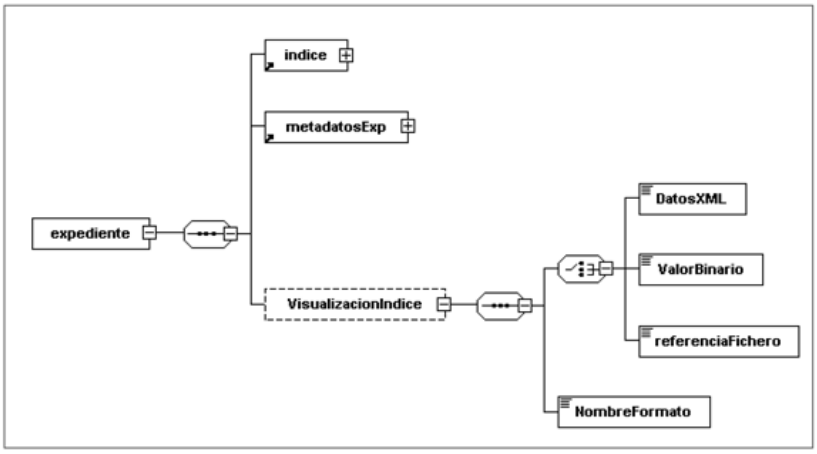
<Órgano>: Véase codificación del metadato "Órgano".

<ID_PRO_específico>: Código alfanumérico que identifica de forma única al procedimiento dentro de los propios de la administración. Cada administración puede diseñar el proceso de generación según susnecesidades, asegurando en cualquier caso su unicidad. Por lo tanto, este ID puede generarse de forma secuencial o bien, ser una réplica del ID utilizado a nivel interno de la administración. (Longitud: 30 caracteres).

## ANEXO II

## Esquemas XML para intercambio de expedientes electrónicos

1. *XSD Expediente electrónico*

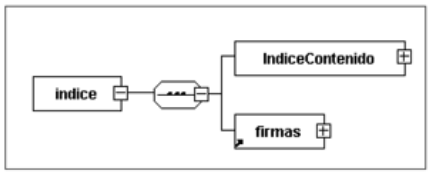



```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:eniexpind="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e"
xmlns:eniexpmeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/metadatos"
xmlns:eniexp="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e"
xmlns:enifile="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD EXPEDIENTE ELECTRONICO ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-
e/IndiceExpedienteEni.xsd"/>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/metadatos" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-
e/metadatos/MetadatosExpedienteEni.xsd"/>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-
e/contenido/contenidoDocumentoEni.xsd"/>
<xsd:element name="expediente" type="eniexp:TipoExpediente"/>
<xsd:complexType name="TipoExpediente">
    <xsd:annotation>
        <xsd:documentation>
```

Para el intercambio de un expediente electrónico, se envía en primer lugar, el índice del expediente. Posteriormente, se enviarán los documentos que lo componen, uno a uno, y siguiendo la distribución reflejada en el contenido del Índice.

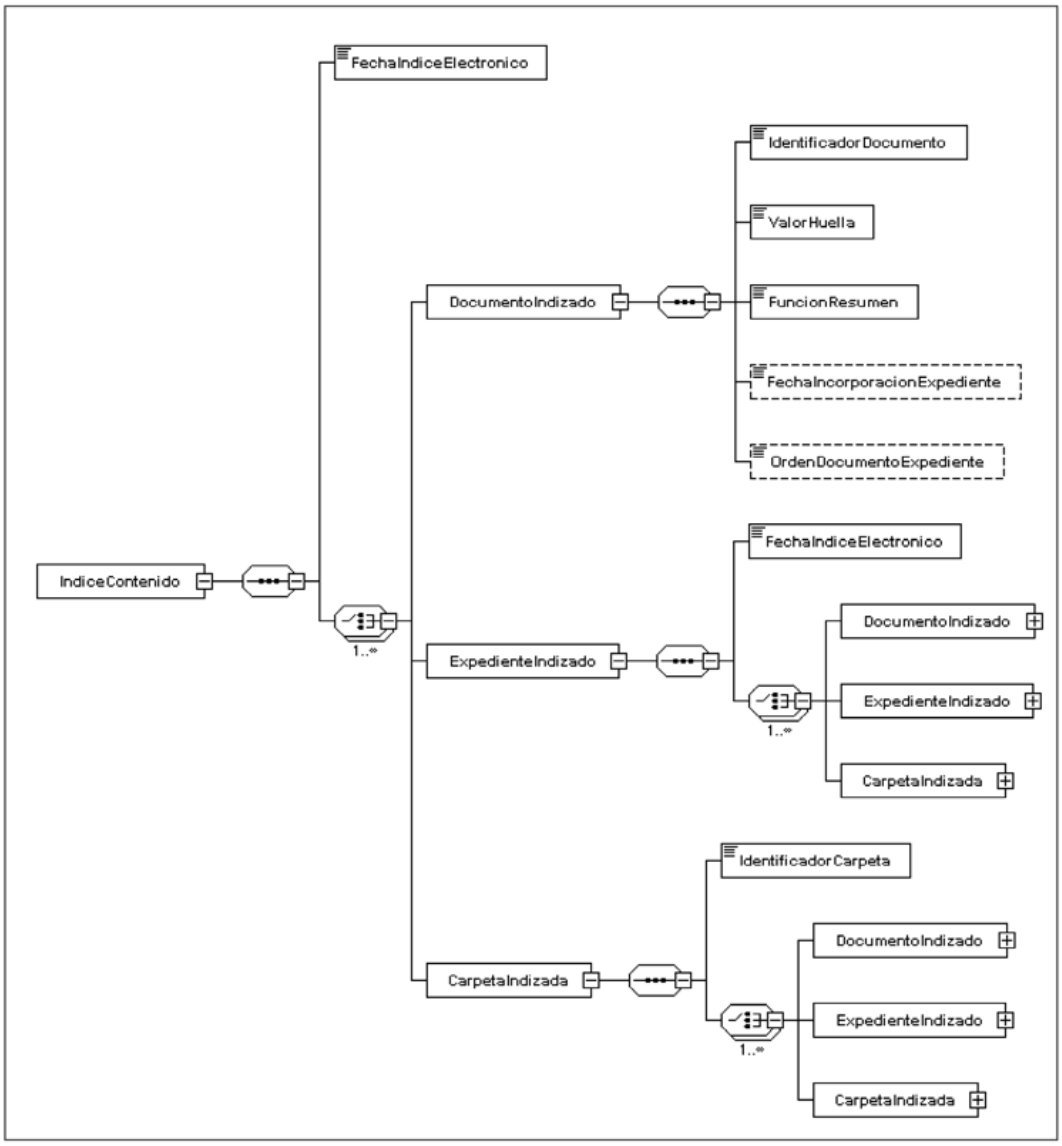
```
</xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
        <xsd:element ref="eniexpind:indice"/>
        <xsd:element ref="eniexpmeta:metadatosExp"/>
        <xsd:element name="VisualizacionIndice" type="enifile:TipoContenido" minOccurs="0" maxOccurs="1"/>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

2. *XSD Índice electrónico del expediente*



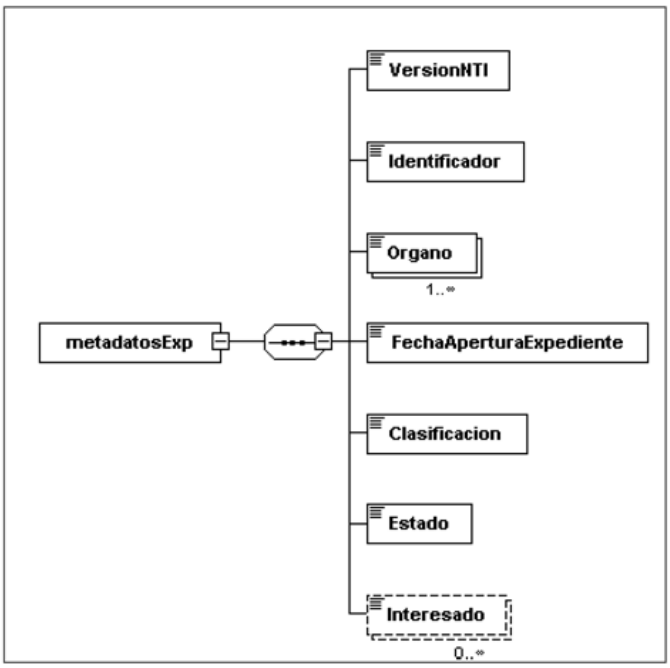

```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma"
xmlns:eniexpind="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e"
xmlns:eniconexpind="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e/contenido" targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
<xsd:documentation xml:lang="es">XSD INDICE EXPEDIENTE ELECTRONICO ENI (v1.0)
</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma/firmasEni.xsd"/>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e/contenido"
schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-
e/contenido/IndiceContenidoExpedienteEni.xsd"/>
<xsd:element name="indice" type="eniexpind:TipoIndice"/>
<xsd:complexType name="TipoIndice">
    <xsd:sequence>
        <xsd:element name="IndiceContenido" type="eniconexpind:TipoIndiceContenido"/>
        <xsd:element ref="enids:firmas">
            <xsd:annotation>
<xsd:documentation>Existirá, al menos, una firma del contenido del índice del expediente electrónico.</xsd:documentation>
            </xsd:annotation>
        </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

3. *XSD Contenido del índice electrónico del expediente*



```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:eniconexpind="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e/contenido" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD CONTENIDO INDICE EXPEDIENTE ELECTRONICO ENI (v1.0) </xsd:documentation>
</xsd:annotation>
<xsd:element name="IndiceContenido" type="eniconexpind:TipoIndiceContenido"/>
<xsd:complexType name="TipoIndiceContenido">
    <xsd:sequence>
        <xsd:element name="FechaIndiceElectronico" type="xsd:dateTime"/>
        <xsd:choice maxOccurs="unbounded">
            <xsd:element name="DocumentoIndizado"
             type="eniconexpind:TipoDocumentoIndizado"/>
            <xsd:element name="ExpedienteIndizado"
             type="eniconexpind:TipoIndiceContenido"/>
            <xsd:element name="CarpetaIndizada" type="eniconexpind:TipoCarpetaIndizada"/>
        </xsd:choice>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
<xsd:complexType name="TipoDocumentoIndizado">
    <xsd:sequence>
        <xsd:element name="IdentificadorDocumento" type="xsd:string"/>
        <xsd:element name="ValorHuella" type="xsd:string"/>
        <xsd:element name="FuncionResumen" type="xsd:string"/>
        <xsd:element name="FechaIncorporacionExpediente" type="xsd:dateTime" minOccurs="0"/>
        <xsd:element name="OrdenDocumentoExpediente" type="xsd:string" minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
<xsd:complexType name="TipoCarpetaIndizada">
    <xsd:sequence>
        <xsd:element name="IdentificadorCarpeta" type="xsd:string"/>
        <xsd:choice maxOccurs="unbounded">
            <xsd:element name="DocumentoIndizado"
             type="eniconexpind:TipoDocumentoIndizado"/>
            <xsd:element name="ExpedienteIndizado"
             type="eniconexpind:TipoIndiceContenido"/>
            <xsd:element name="CarpetaIndizada" type="eniconexpind:TipoCarpetaIndizada"/>
        </xsd:choice>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

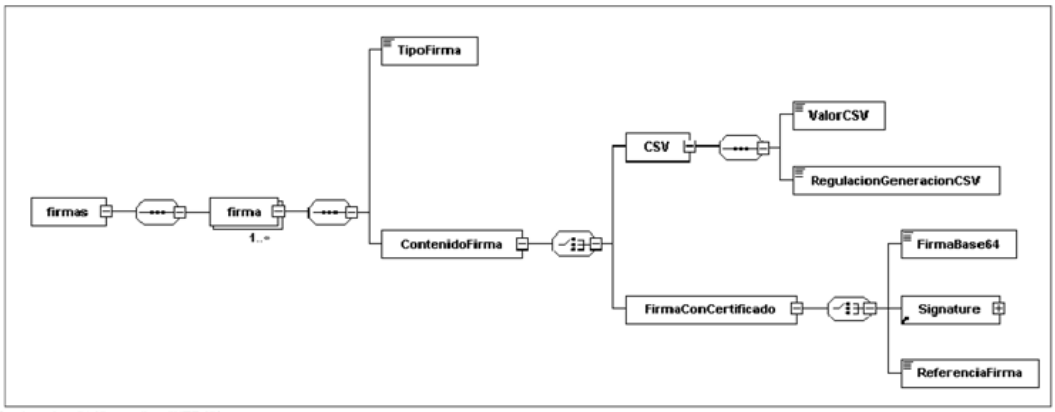
4. *XSD Metadatos del expediente electrónico*




```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:eniexpmeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/metadatos"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/metadatos"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
<xsd:documentation xml:lang="es">XSD METADATOS EXPEDIENTE ELECTRONICO ENI (v1.0) </xsd:documentation>
</xsd:annotation>
<xsd:element name="metadatosExp" type="eniexpmeta:TipoMetadatos"/>
<xsd:complexType name="TipoMetadatos">
    <xsd:sequence>
        <xsd:element name="VersionNTI" type="xsd:anyURI"/>
        <xsd:element name="Identificador" type="xsd:string"/>
        <xsd:element name="Organo" type="xsd:string" minOccurs="1" maxOccurs="unbounded"/>
        <xsd:element name="FechaAperturaExpediente" type="xsd:dateTime"/>
        <xsd:element name="Clasificacion" type="xsd:string"/>
        <xsd:element name="Estado">
```

```
            <xsd:annotation>
                <xsd:documentation xml:lang="es">
                - E01 - Abierto.
                - E02 - Cerrado.
                - E03 - Índice para remisión cerrado.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:complexType>
                <xsd:simpleContent>
                    <xsd:extension base="eniexpmeta:enumeracionEstados"/>
                </xsd:simpleContent>
            </xsd:complexType>
        </xsd:element>
        <xsd:element name="Interesado" type="xsd:string" minOccurs="0" maxOccurs="unbounded">
            <xsd:annotation>
<xsd:documentation xml:lang="es">Obligatorio cumplimentar en caso de que exista al menos un interesado.</xsd:documentation>
            </xsd:annotation>
        </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>

<!-- Enumeración de Estados del expediente -->
<xsd:simpleType name="enumeracionEstados">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="E01"/>
        <xsd:enumeration value="E02"/>
        <xsd:enumeration value="E03"/>
    </xsd:restriction>
</xsd:simpleType>
</xsd:schema>
```

5. *XSD Firmas*




```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma "
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD FIRMAS ELECTRONICAS ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
 schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
<xsd:element name="firmas" type="enids:firmas"/>
<xsd:complexType name="firmas">
    <xsd:sequence>
        <xsd:element name="firma" type="enids:TipoFirmasElectronicas" minOccurs="1" maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="TipoFirmasElectronicas">
    <xsd:sequence>
        <xsd:element name="TipoFirma">
            <xsd:annotation>
                <xsd:documentation xml:lang="es">
                    - TF01 - CSV.
                    - TF02 - XAdES internally detached signature.
                    - TF03 - XAdES enveloped signature.
                    - TF04 - CAdES detached/explicit signature.
                    - TF05 - CAdES attached/implicit signature.
```

```
                - TF06 - PAdES.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:simpleType>
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="TF01"/>
                <xsd:enumeration value="TF02"/>
                <xsd:enumeration value="TF03"/>
                <xsd:enumeration value="TF04"/>
                <xsd:enumeration value="TF05"/>
                <xsd:enumeration value="TF06"/>
            </xsd:restriction>
        </xsd:simpleType>
    </xsd:element>
    <xsd:element name="ContenidoFirma">
        <xsd:complexType>
            <xsd:choice>
                <xsd:element name="CSV">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="ValorCSV" type="xsd:string"/>
                            <xsd:element name="RegulacionGeneracionCSV" type="xsd:string"/>
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
                <xsd:element name="FirmaConCertificado">
                    <xsd:complexType>
                        <xsd:choice>
                            <xsd:element name="FirmaBase64" type="xsd:base64Binary"/>
                            <xsd:element ref="ds:Signature"/>
                            <xsd:element name="ReferenciaFirma">
                                <xsd:annotation>
                                <xsd:documentation  xml:lang="es"> Referencia interna al fichero que incluye la firma. </xsd:documentation>
                                </xsd:annotation>
                        </xsd:element>
                        </xsd:choice>
                    </xsd:complexType>
                </xsd:element>
            </xsd:choice>
        </xsd:complexType>
    </xsd:element>
</xsd:sequence>
<xsd:attribute name="Id" type="xsd:ID" use="optional"/>
<xsd:attribute name="ref" type="xsd:string" use="optional">
    <xsd:annotation>
        <xsd:documentation xml:lang="es">Almacena el identificador del nodo que se está firmando. En caso de firmas multinodo, se incluirá una lista separada por comas de los identificadores
        de los nodos firmados. </xsd:documentation>
    </xsd:annotation>
</xsd:attribute>
</xsd:complexType>
</xsd:schema>
```

# § 17

## Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 266, de 3 de noviembre de 2016
Última modificación: sin modificaciones
Referencia: BOE-A-2016-10146

El Esquema Nacional de Interoperabilidad se establece en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que sustituye al apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia, en el marco, entre otras normas, de la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma y sello, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y reutilización de la información del sector público; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, según se establece en el artículo 29 del Esquema Nacional de Interoperabilidad.

En particular, la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración se aprobó mediante Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, para responder a lo previsto en el artículo 18 del citado Real Decreto 4/2010, de 8 de enero, sobre la interoperabilidad en materia de firma y sello electrónicos y de certificados.

Posteriormente, la evolución de las tecnologías de aplicación, la experiencia derivada de la aplicación de la citada Norma Técnica de Interoperabilidad, la entrada en vigor de la citada Ley 40/2015, de 1 de octubre, y la evolución del contexto regulatorio europeo, particularmente por razón del Reglamento n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, y su normativa de desarrollo, hacen necesario una actualización de esta Norma Técnica de Interoperabilidad.

La Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la Administración, que sustituye a la anterior denominada de Política de Firma Electrónica y de certificados de la Administración, establece el conjunto de criterios para el desarrollo o adopción de políticas de firma y sello electrónicos basada en certificados por parte de las Administraciones públicas. Para ello, define el contenido de una política de firma electrónica y sello electrónico basados en certificados, especificando las características de las reglas comunes, como formatos, uso de algoritmos, creación y validación de firma para documentos electrónicos, así como de las reglas de confianza en certificados electrónicos, sellos de tiempo y firmas longevas.

Las condiciones establecidas en esta norma persiguen establecer un marco para la definición de políticas de firma y sello electrónicos basada en certificados alineada con actos europeos recientes como la Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, compatible a su vez con sistemas de firma electrónica ya implantados.

La presente actualización de la norma técnica se ha elaborado con la participación de todas las Administraciones Públicas a las que les es de aplicación, ha sido informada favorablemente por el Comité de Dirección de Tecnologías de la Información y Comunicaciones y por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la Administración, que sustituye completamente a la anterior Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración, y cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la Administración que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## NORMA TÉCNICA DE INTEROPERABILIDAD DE POLÍTICA DE FIRMA Y SELLO ELECTRÓNICOS Y DE CERTIFICADOS DE LA ADMINISTRACIÓN

*I Consideraciones generales*

I.1 Objeto.

1. La Norma Técnica de Interoperabilidad (en adelante, NTI) de Política de firma y sello electrónicos y de certificados de la Administración tiene por objeto establecer el conjunto de criterios comunes asumidos por la Administración pública en relación con la autenticación y el reconocimiento mutuo de firmas electrónicas y sellos electrónicos basados en certificados

electrónicos cualificados o reconocidos y que, como tales, serán desarrollados y consolidados a través de las políticas de firma y sello electrónicos basados en certificados.

2. El objetivo final de esta NTI es facilitar el uso de firmas electrónicas y sellos electrónicos seguros e interoperables entre las distintas organizaciones de la Administración pública.

I.2 Ámbito de aplicación.

1. El contenido de esta NTI será de aplicación para el desarrollo o adopción de políticas de firma y sello electrónicos basada en certificados por parte de cualquier órgano de la Administración pública o Entidad de Derecho Público vinculada o dependiente de aquélla (en adelante, organizaciones) según el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

2. Las políticas de firma y sello harán referencia a un contexto concreto de carácter horizontal donde sea necesario normalizar aspectos de las firmas electrónicas de los Documentos Electrónicos Administrativos para garantizar la interoperabilidad, no a una Administración u organismo particular. Para establecer los aspectos técnicos de las firmas dentro de una Administración u organismos concreto, se optará por la generación de instrucciones técnicas internas, procedimientos o directrices de aplicaciones, que en todo caso deberán ajustarse a lo establecido por el Esquema Nacional de Seguridad.

*II La política de firma y sello electrónicos*

II.1 Definición y contenido.

1. Según la definición del Real Decreto 4/2010, de 8 de enero, una política de firma electrónica es el «conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma». Es de aplicación tanto a las firmas como a los sellos electrónicos.

2. Una política de firma y sello electrónicos y de certificados definirá:

a) Los procesos de creación, validación y conservación de firmas electrónicas y sellos electrónicos.

b) Características y requisitos de los sistemas de firma electrónica, sellos electrónicos, certificados y sellos de tiempo.

3. Toda política de firma y sello electrónicos basada en certificados incluirá:

a) Definición del alcance y ámbito de aplicación, que concretará su relación con otras políticas existentes, marco o particulares, así como la identificación de los actores involucrados y los usos de la firma electrónica y sello electrónico.

b) Datos para la identificación del documento y del responsable de su gestión.

c) Reglas comunes para el firmante, el creador del sello, y el verificador de la firma o sello electrónicos que incluirán:

i. Formatos admitidos de firma electrónica y sello electrónico, y reglas de uso de algoritmos.

ii. Reglas de creación de firma o sello electrónicos.

iii. Reglas de validación de firma o sello electrónicos.

d) Reglas de confianza, que incluirán los requisitos establecidos para certificados, sellos de tiempo y firmas longevas.

e) Otras reglas opcionales a fijar por cada organización, como podrán ser:

i. Reglas específicas de compromisos que cada organización podrá establecer para cada uno de los servicios que presta, estableciendo requisitos específicos necesarios para que la firma sea válida en cada caso.

ii. Reglas de certificados de atributos mediante las que cada organización podrá establecer información adicional a añadir a los certificados digitales en función de sus necesidades y del contexto.

f) Definición de condiciones para el archivado y custodia de firmas electrónicas.
g) Descripción de consideraciones de gestión de la política que se aplicarán a dicho documento.

II.2 Datos identificativos de la política.

1. El documento de política de firma y sello incluirá la siguiente información para su identificación:

a) Nombre del documento.
b) Versión.
c) Identificador (OID Object IDentifier) de la política.
d) URI (Uniform Resource Identifier) de referencia de la política.
e) Fecha de expedición.
f) Ámbito de aplicación.

2. La política de firma y sello incluirá la definición de su periodo de validez y las consideraciones respecto a los periodos de transición que procedan.
3. Para la identificación de su gestor, la política de firma y sello electrónicos basada en certificados incluirá:

a) Nombre del gestor de la política.
b) Dirección de contacto.
c) OID del gestor de la política de firma.

II.3 Actores involucrados en la firma electrónica.

Los actores involucrados en el proceso de creación y validación de una firma electrónica serán:

a) Firmante: Una persona física que crea una firma electrónica utilizando datos de creación de firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
b) Creador de un sello: Una persona jurídica que crea un sello electrónico.
c) Verificador: Entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la política de firma y sello concreta por la que se rige la plataforma de relación electrónica o el servicio concreto al que se esté invocando. Podrá ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.
d) Prestador de servicios de confianza (PSC): Una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza.
e) Emisor y gestor de la política de firma: Entidad que se encarga de generar y gestionar el documento de política de firma y sello, por el cual se deben regir el firmante, el verificador y los prestadores de servicios en los procesos de generación y validación de firma electrónica.

En este documento que utilizará el término ‘firmante’, tanto para referirse al firmante como al creador de un sello. Puede tratarse de un proceso de actuación administrativa automatizada.
Se usará el término ‘firma’ tanto para referirse a la firma electrónica como a sello electrónico.

II.4 Usos de la firma electrónica.

Las políticas de firma y sello electrónicos podrán definir condiciones para la aplicación de una firma electrónica basada en certificados con los siguientes propósitos:

a) Firma de transmisiones de datos, como herramienta para proporcionar seguridad al intercambio, garantizando la autenticación de los actores involucrados en el proceso, la integridad del contenido del mensaje de datos enviado y el no repudio de los mensajes en una comunicación telemática.

b) Firma de contenido como herramienta para garantizar la autenticidad, integridad y no repudio de aquel, con independencia de que forme parte de una transmisión de datos.

II.5 Interacción con otras políticas.

1. Las Administraciones Públicas se acogerán preferentemente a la Política Marco de Firma Electrónica basada en Certificados

a. Cada organización valorará la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de utilizar una política marco existente.
b. Las Administraciones Públicas podrán aprobar otras políticas de firma y sello electrónicos dentro de sus ámbitos competenciales si las características particulares de los procedimientos administrativos bajo su competencia lo hacen necesario. Las políticas de firma y sello particulares estarán orientadas a un contexto concreto, de carácter horizontal, no a una organización concreta. En el caso de que en una organización se deseen normalizar únicamente aspectos técnicos de las firmas electrónicas, se optará por otro instrumento distinto de una Política de firma y sello, como instrucciones técnicas internas o directrices de aplicaciones.
c. Serán aprobadas con informe favorable del Comité Sectorial de Administración Electrónica y del Comité Ejecutivo de la Comisión de Estrategia TIC, una vez verificada su interoperabilidad con la Política Marco de Firma Electrónica basada en Certificados.
d. Con objeto de permitir la interoperabilidad de las firmas electrónicas acordes a políticas, las políticas que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Dirección de Tecnologías de la Información y las Comunicaciones del Ministerio de Hacienda y Administraciones Públicas.

2. La definición del alcance y ámbito de aplicación de una política de firma y sello electrónicos se realizará considerando su interacción con otras políticas de firma y sello electrónicos, y asegurando que:

a) Su desarrollo es interoperable con la política marco, en caso de políticas de firma y sello particulares.
b) Define las condiciones de utilización y convivencia con otras políticas particulares, si se trata de una política marco.

3. En toda política de firma y sello electrónicos se asegurará que:

a) Las extensiones o restricciones establecidas para las reglas de creación o validación de firma atienden a la validación de los formatos de firma establecidos en esta NTI y política marco si procede, de forma que se garantice la interoperabilidad entre las diferentes organizaciones.
b) Incluye, si procede, la referencia a la URL de la política marco de firma electrónica en la que se inscribe, con indicación expresa de la versión.
c) Las firmas que se generen siguiendo políticas marco o particulares, incluyen un campo donde se indique de forma explícita la política a la que pertenecen.
d) Para que otras aplicaciones puedan interpretar las reglas de una política particular correctamente, dicha política está disponible en formato XML (eXtensible Markup Language) y ASN.1 (Abstract Syntax Notation One).

II.6 Gestión de la política de firma y sello.

1. La política de firma y sello electrónicos incluirá la descripción básica de su proceso de gestión, estableciendo las directrices para su mantenimiento, actualización y publicación, e identificando al responsable de llevar a cabo estas tareas.
2. El gestor de la política de firma mantendrá actualizada la versión de la política de firma y sello atendiendo a:

a) Modificaciones motivadas por necesidades propias de la organización.
b) Cambios en políticas relacionadas.
c) Cambios en los certificados electrónicos emitidos por los prestadores de servicios de certificación referenciados en la política de firma y sello.

3. Para facilitar la validación de firmas electrónicas creadas atendiendo a versiones anteriores de una política, se podrá mantener un repositorio con el historial de versiones anteriores que provea la ubicación de cada versión.

II.7 Archivado y custodia.

1. Atendiendo a las necesidades y normativa específicas de su ámbito, las políticas de firma y sello podrán contemplar la definición de condiciones y responsabilidades para el archivado y custodia de las firmas electrónicas en sus diferentes aplicaciones.

2. Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, se podrán utilizar:

a) Firmas longevas mediante las que se añadirá información del estado del certificado asociado, incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza, aplicando las reglas de confianza para firmas longevas descritas en el subapartado IV.3.

b) Otros métodos técnicos que impedirán la modificación de la firma para la que se ha verificado su validez, de acuerdo a los requisitos establecidos en la política de firma y sello correspondiente, y que habrá sido almacenada en un sistema en un momento del tiempo determinado. Todos los cambios que se realicen sobre el sistema en el que se encuentra almacenada la firma podrán auditarse para asegurar que dicha firma no ha sido modificada. Los requisitos de seguridad de dichos sistemas cumplirán con las condiciones de los niveles de seguridad establecidos por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3. Cada política de firma y sello definirá un servicio para mantener las evidencias de validez de las firmas longevas y gestionar la actualización de las firmas y sellos. Dicho servicio especificará los mecanismos y condiciones bajo los que se archiva y custodia tanto la propia firma o sello como los certificados e informaciones de estado utilizadas en su validación.

4. El almacenamiento de los certificados y las informaciones de estado podrá realizarse dentro del fichero resultante de la firma electrónica o en un depósito específico:

a) En caso de almacenar los certificados y las informaciones de estado dentro de la firma, se sellarán también dichas informaciones, siguiendo las modalidades de firmas recogidas en la «Decisión de Ejecución UE 2015/1506 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público», o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior».

b) Si los certificados y las informaciones de estado se almacenan en un depósito específico, se sellarán de forma independiente.

5. La protección de la firma/sello electrónico frente a la posible obsolescencia de los algoritmos y el aseguramiento de sus características a lo largo del tiempo de validez, se realizará a través de uno de los siguientes procesos:

a) Utilización de mecanismos de resellado de tiempo, para añadir, cuando el anterior sellado este próximo a su caducidad, un sello de fecha y hora de archivo con un algoritmo más robusto.

b) Se recomienda utilizar mecanismos de resellado/refirma, en el caso de obsolescencia de los algoritmos o formatos, con un algoritmo más robusto.

c) Almacenamiento de la firma electrónica en un depósito seguro, que garantice la protección de la firma contra modificaciones y asegurando la fecha exacta en que se guardó la firma electrónica, y en la que se comprobó la autenticidad y vigencia de los elementos que la conforman.

d) Otros sistemas que garanticen la preservación de las firmas y sellos a largo plazo con certeza de la comprobación de su validez en el momento más próximo que sea posible respecto a su generación o admisión. Estos sistemas adicionales deberán estar descritos

minuciosamente en el documento de gestión de política de custodia documental de la entidad, con indicación de los plazos en los que los sistemas estuvieron vigentes y los archivos a los que estos sistemas se aplicaron, especialmente para el caso de valoración documental a largo plazo por especialistas en archivos.

6. La definición de medidas y procedimientos para archivado y custodia de firmas/sellos electrónicos se realizará atendiendo con proporcionalidad a los diferentes usos de la firma electrónica contemplados en el alcance y ámbito de aplicación de la política.

7. Para archivado y gestión de documentos electrónicos firmados o sellados, se atenderá a lo establecido en la NTI de Política de gestión de documentos electrónicos.

*III Reglas comunes*

III.1 Reglas comunes.

1. Las reglas comunes permitirán establecer responsabilidades respecto a la firma/sello electrónicos sobre la persona o entidad que crea la firma y la persona o entidad que la verifica, definiendo los requisitos mínimos que deben presentarse, debiendo estar firmados si son requisitos para el firmante, o no firmados si son requisitos para el verificador.

2. Estas reglas se definirán en base a los formatos de firma/sello electrónico admitidos, teniendo en cuenta los diferentes usos de la firma electrónica basada en certificados, al uso de algoritmos y a los procesos de creación y validación de firma y sello.

III.2 Formatos admitidos de firma electrónica.

1. Los formatos admitidos por las organizaciones para las firmas/sellos electrónicos basadas en certificados electrónicos, se ajustarán a:

a) la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior».

b) lo establecido en la NTI de Catálogo de estándares.

c) los formatos CAdES, XAdES y PAdES en las versiones establecidas en la Norma Técnica de Interoperabilidad de Política de firma del 2011.

2. Los formatos de firma/sello electrónico serán

a) Si procede, interoperables con la política marco en la que se basan.

III.3 Formatos de firma electrónica de transmisiones de datos.

1. La firma electrónica de transmisiones de datos estará basada en estándares recogidos en la NTI de Catálogo de estándares, siendo responsabilidad del emisor y gestor de la política la definición de las consideraciones concretas a aplicar por cada organización.

2. Cada política definirá las versiones soportadas así como los cambios en aquellas que pueden provocar una actualización de dicha política.

III.4 Formatos de firma/sello electrónica de contenido.

1. Los formatos para la firma/sello electrónica de contenido se ajustarán a la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) 910/2014»

2. Por compatibilidad con las políticas de firma anteriores, se permitirán aunque no se recomiendan los siguientes formatos::

a) XAdES (XML Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2.

b) CAdES (CMS Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7.4.

c) PAdES (PDF Advanced Electronic Signatures), según la especificación técnica ETSI TS 102 778-3.

3. El perfil mínimo de formato que se utilizará para la generación de firmas de contenido en el marco de una política será «-EPES», esto es, clase básica (BES) añadiendo

información sobre la política de firma y sello. En cualquier caso, cada organización podrá definir en su política de firma y sello las consideraciones adicionales que considere respecto a la interpretación y utilización de diferentes perfiles y clases de los formatos siempre en consonancia con lo establecido en esta NTI.

4. Las organizaciones aplicarán consideraciones de casos particulares para firma de contenido, al menos, en los siguientes casos:

a) Los documentos electrónicos a los que se aplique firma/sello basada en certificados de cara a su intercambio se ajustarán a las especificaciones de formato y estructura establecidas en la NTI de Documento electrónico.

El formato de firma basada en certificados que acompaña a un documento electrónico se reflejará en el metadato mínimo obligatorio definido en la NTI de Documento electrónico 'Tipo de firma', que, en este caso, podrá tomar uno de los siguientes valores:

i. XAdES internally detached signature.
ii. XAdES enveloped signature.
iii. CAdES detached/explicit signature.
iv. CAdES attached/implicit signature.
v. PAdES.
vi. XAdES (Decision 1506) detached
vii. XAdES (Decision 1506) enveloped
viii. CAdES (Decision 1506) detached
ix. CAdES (Decision 1506) attached
x. PAdES (Decision 1506)

b) La firma/sello de facturas electrónicas según el formato «Facturae» se realizará conforme a lo regulado por la Orden PRE/2971/2007, de 5 de octubre, o normativa que la sustituya.

III.5 Reglas de uso de algoritmos.

1. La política de firma y sello especificará las reglas de uso de algoritmos en los diferentes formatos así como la longitud de las claves asociadas a aquéllos de forma proporcional a las necesidades detectadas en los diferentes usos de la firma/sello electrónicos, cumpliendo en cualquier caso lo establecido en la NTI de Catálogo de estándares y lo previsto en las normas que se definan en aplicación del Reglamento (UE) 910/2014.

2. Para los entornos de seguridad regulados por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/ 2015, de 1 de octubre, de Régimen Jurídico del Sector Público, de aplicación en los procedimientos de administración electrónica, se ajustarán a la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) 910/2014» o las especificaciones técnicas publicadas por los organismos de Estandarización Europeos. La definición de usos de algoritmos podrá contemplar diferentes posibilidades según lo establecido en las guías aplicables, como la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía, las normas ETSI TS 119 312 'Criptographic Suites for secure electronic signatures', o aquellas que las sustituyan.

3. Para los entornos de alta seguridad, de acuerdo con el criterio del Centro Criptológico Nacional (CCN) serán de aplicación las recomendaciones revisadas de la CCN-STIC 405 así como en la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía.

III.6 Reglas de creación de firma electrónica.

1. Las políticas de firma y sello definirán las condiciones particulares bajo las que, en su ámbito, se generará la firma electrónica.

2. Las plataformas que presten el servicio de creación de firma electrónica proporcionarán las funcionalidades necesarias para soportar un proceso de creación de firmas y sellos basado en los siguientes puntos:

a) Selección por parte del usuario firmante del fichero, formulario u otro objeto binario para ser firmado. Los formatos de ficheros atenderán a lo recogido en la NTI de Catálogo de estándares.

El firmante se asegurará de que el fichero que se quiere firmar no contiene contenido dinámico que afecte a su validez y que pudiese modificar el resultado de la firma/sello a lo largo del tiempo.

b) El servicio de firma electrónica ejecutará las siguientes verificaciones previas a la creación de la firma:

i. La firma/sello electrónicos pueden ser validados para el formato del fichero específico que va a ser firmado.

ii. Validez del certificado, comprobando si el certificado ha sido revocado, o suspendido, si entra dentro de su periodo de validez, y la validación de la cadena de certificación, incluyendo la validación de todos los certificados en la cadena, y de su vigencia y estado de no revocación, y si el certificado ha sido expedido por un Prestador de Servicios de Confianza Cualificado, incluido en la TSL del país emisor.

Si alguna de estas verificaciones es errónea, el proceso de firma se interrumpirá.

Si no fuese posible realizar estas comprobaciones en el momento de la firma, será necesario, en todo caso, que los sistemas receptores de la firma asuman dicha validación, antes de aceptar el fichero, formulario u otro objeto binario firmado.

c) El servicio creará un fichero con la firma/sello según corresponda en función del formato utilizado.

En el momento de la firma, se incluirá la referencia del identificador único de la versión del documento de política de firma y sello electrónicos en el que se ha basado su creación.

3. La vinculación del firmante se establecerá a través de etiquetas que, incluidas bajo la firma, y definidas según los estándares correspondientes (XAdES, CAdES y/o PAdES), proporcionarán la siguiente información complementaria a ésta:

a) Fecha y hora de firma, que podrá ser meramente indicativa en función de cómo se haya generado la firma.

b) Certificado del firmante.

c) Cadena de validación.

d) Política de firma y sello sobre la que se basa el proceso de generación de firma electrónica.

e) Formato del objeto original.

4. Como datos opcionales, la firma/sello electrónicos podrá incluir:

a) Lugar geográfico donde se ha realizado la firma del documento.

b) Rol de la persona firmante en la firma electrónica.

c) Acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, etc.).

d) Sello de tiempo sobre algunos o todos los objetos de la firma.

5. En caso de creación de firmas/sellos electrónicos por distintos firmantes sobre un mismo objeto, donde el segundo firmante ratifica la firma del primero se utilizará la etiqueta correspondiente, CounterSignature, para contabilizarlas.

6. En el caso de que las múltiples firmas/sellos se realicen al mismo nivel, cada una de ellas se representará como una firma independiente.

III.7 Reglas de validación de firma/sello electrónicos.

1. Las políticas de firma y sello definirán las condiciones particulares bajo las que, en su ámbito, será posible validar la firma electrónica de un documentosiguiendo los requisitos establecidos en el artículo 32.1 del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

2. En el caso de documentos electrónicos, para acceder a la visualización de la firma/sello, el usuario podrá presentar dicho documento electrónico, que contenga los datos,

metadatos y firmas/sellos, en una sede electrónica o en otros sistemas generales que proporcionen herramientas de reproducción de documentos electrónicos.

3. Las condiciones mínimas que se producirán para la validación de la firma/sello serán las siguientes:

a) Garantía de que la firma es válida para el fichero específico que está firmado.

b) Validez de los certificados:

i. El instante de tiempo que se tomará como referencia para la validación será:

1) El momento en que se produjo la firma/sello si se da alguno de los siguientes supuestos:

a. los servicios de los prestadores facilitan los históricos de estado de los certificados y la firma/sello lleva un sello de tiempo válido en el momento de la verificación.

b. se trata de firmas/sellos longevos que incluyen las evidencias de la validez de la firma electrónica en el momento de la generación o primera validación, y dichas evidencias se encuentran selladas con un sello de tiempo válido.

2) En otros casos, el momento de la validación.

ii. Se comprobará que los certificados no fueron revocados ni suspendidos y que no han expirado.

iii. Se comprobará la validez de toda la cadena de certificación, incluyendo todos los certificados que la componen, con independencia de que éstos se encuentren incluidos en la propia firma o no.

iv. Se verificará que el certificado ha sido expedido por un prestador de servicios de certificación de confianza bajo una Declaración de Prácticas de Certificación que cumplirá la normativa y estará incluido en la política de firma y sello aplicable, y ha sido expedido por un Prestador de Servicios de Confianza Cualificado, incluido en la TSL del país emisor.

v. Verificación, si existen y si así lo requiere la política de la plataforma de relación electrónica o un servicio concreto de dicha plataforma, de los sellos de tiempo de los formatos implementados, incluyendo la verificación de los periodos de validez de los sellos de tiempo.

4. Para validar la firma electrónica se considerará la siguiente información:

a) Fecha y hora de la firma/sello: Si se ha realizado el sellado de tiempo, el sello de tiempo más antiguo dentro de la estructura de la firma se utilizará para determinar la fecha de la firma/sello. En caso de que no existan sellos de tiempo, la fecha y hora de la firma tendrán carácter indicativo, pero no se utilizarán para determinar el momento en que se realizó la firma. En caso de que no existan sellos de tiempo en la firma, la validación del certificado se realizará en el momento de la validación de la firma/sello.

b) Certificado del firmante. Este campo se utilizará para verificar el estado del certificado, y en su caso la cadena de certificación, en la fecha de la generación de la firma/sello.

c) Política de firma y sello sobre la que se basa el proceso de generación de firma electrónica. Se utilizará para identificar, mediante su hash y su identificador (OID), que la política de firma y sello que se ha utilizado para la generación de la firma se corresponde con la que se utilizará para el servicio en cuestión.

Esta validación de la política de firma y sello, implicará que el verificador dispondrá de los medios para verificar las condiciones impuestas en la política de firma y sello concreta. La disponibilidad de la política de firma y sello en un formato interpretable por medios automatizados (XML o ASN.1) y siguiendo los estándares europeos de representación de políticas de firma, indicada en el epígrafe 3.d del subapartado II.5 de esta NTI, facilitará la labor de las aplicaciones receptoras de firmas electrónicas en aplicar distintas políticas de firma y sello.

5. Si se han realizado varias firmas/sellos sobre un mismo documento, se seguirá el mismo proceso de verificación que con la primera firma/sello, comprobando cada firma o la etiqueta CounterSignature en el campo de propiedades no firmadas, donde se informa de los refrendos de firma generados.

6. El encargado de la verificación de la firma/sello podrá definir sus procesos de validación y de archivado, siempre en consonancia con los requisitos de la política de firma y

sello a la que se ajuste el servicio y con lo establecido en la NTI de Política de gestión de documentos electrónicos.

7. Para la verificación del estado de los certificados en el caso de formatos de firma longeva, la validez de la firma/sello vendrá determinada por la validez del sello de tiempo de las evidencias de la validación incluidas en la firma. En estos casos la validez de la firma/sello a lo largo del tiempo se mantendrá resellando la firma/sello antes de la caducidad del certificado de la TSA (Autoridad de sellado de tiempo) que realizó el sello de tiempo anterior, de forma que siempre sea posible verificar que en el momento en que se realizó la firma/sello, el certificado era válido.

8. En el caso de validación por un tercero, el validador ofrecerá a la parte usuaria el resultado correcto del proceso de validación.

*IV Reglas de confianza*

IV.1 Reglas de confianza para los certificados electrónicos.

1. Las políticas de firma y sello, marco o particulares, podrán fijar limitaciones y restricciones específicas para los certificados electrónicos que admiten en cada uno de los servicios que corresponda, si el uso destinado del certificado establecido en su Política de Certificación no está acorde al ámbito de la Política de firma y sello, siempre en consideración de la normativa aplicable en cada caso.

2. Se presumirán válidos los certificados cualificados que usen los ciudadanos en las firmas y sellos electrónicos. Si una administración apreciara algún aspecto que cuestionara esta validez lo hará saber al ciudadano que dispondrá del plazo previsto en la normativa de procedimiento administrativo para subsanar lo que corresponda o ratificar por otra vía los documentos firmados electrónicamente. El firmante no podrá alegar que ha utilizado una firma inválida con arreglo a una determinada Declaración de Prácticas de Certificación como condición en la que se base un recurso de nulidad o anulabilidad de un acto.

3. Los certificados válidos para ejecutar la firma/sello electrónicos de contenido serán los certificados electrónicos cualificados de firma y sello según el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

4. La relación de prestadores de servicios de certificación que emiten certificados electrónicos cualificados se consultará en la TSL (Lista de servicios de confianza) publicada en la sede electrónica del Ministerio de Industria, Energía y Turismo y en las TSL del resto de países de la UE, de conformidad con la Decisión de Ejecución UE 2015/1505 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

5. La política de firma y sello electrónicos podrá establecer el período de precaución o de gracia que corresponda aplicar para la validación de los certificados. Este periodo podrá ser, desde el momento en que se realiza la firma o el sellado de tiempo, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs (Certificate Revocation Lists) o el tiempo máximo de actualización del estado del certificado en el servicio OCSP (Online Certificate Status Protocol). Esta definición tendrá en cuenta también la posibilidad de que estos tiempos varíen según el Prestador de Servicios de Certificación.

6. El verificador validará los certificados electrónicos en base a los procesos de validación y archivado definidos en la política de firma y sello a la que se ajuste el servicio en cada caso.

IV.2 Reglas de confianza para sellos de tiempo.

1. Los sellos cualificados de tiempo cumplirán los indicados en el artículo 42.1 del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las

transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

2. Los elementos básicos de un sello cualificado de tiempo serán los indicados en las Normas Europeas de estandarización:

a) ETSI EN 319 422 V1.1.1Time-stamping protocol and time-stamp token profiles.

b) ETSI EN 319 421 V1.1.1 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

O en las que las sustituyan.

3. El sellado de tiempo y la información de validación podrán ser añadidos por el emisor, el receptor o un tercero y se incluirán como propiedades no firmadas en los campos correspondientes según el formato de firma utilizado.

4. En la política de firma y sello se establecerán las condiciones según las que determinar los sellos de tiempo admitidos atendiendo a sus necesidades particulares, y en base a la normativa y legislación vigente. Esto incluye el establecimiento del tiempo máximo aceptable para realizar el sellado de tiempo, anterior, en cualquier caso, a la caducidad del certificado.

IV.3 Reglas de confianza para firmas longevas.

1. En el caso de firmas longevas, el firmante o el verificador de la firma incluirá un sello de tiempo que permita garantizar que el certificado era válido en el momento en que se realizó la firma. En el caso de que sea incluida por el firmante, se podrá realizar una vez haya trascurrido el periodo de precaución o periodo de gracia.

2. Para la conversión de una firma electrónica a firma electrónica longeva:

a) Se verificará la firma electrónica, validando la integridad de la firma acorde a las reglas de validación de firma de electrónica del epígrafe III.7.

b) Se realizará un proceso de completado de la firma electrónica que consistirá en la obtención y almacenamiento de las referencias a:

i. Certificados: Incluyendo los certificados del firmante y de la cadena de certificación tanto del firmante como del sello de tiempo.

ii. Informaciones de estado de los certificados, CRLs o las respuestas OCSP.

c) Aplicación del sellado de tiempo a las referencias a los certificados y a las informaciones de estado.

3. Para la incorporación a la firma de la información completa de validación, se usará validación mediante CRLs u OCSP.

4. Las políticas de firma y sello contemplarán la definición de formatos y consideraciones de uso de firmas longevas conforme a las necesidades específicas de su ámbito de aplicación y a la normativa específica aplicable.

# § 18

## Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 178, de 26 de julio de 2012
Última modificación: sin modificaciones
Referencia: BOE-A-2012-10049

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, la norma relativa a la intermediación de datos responde a lo previsto en el artículo 9 de la Ley 11/2007, de 22 de junio, y en el artículo 8 del citado Real Decreto 4/2010, de 8 de enero, sobre el acceso y utilización de servicios de intercambio de datos y documentos entre Administraciones Públicas; definiendo un modelo para el intercambio intermediado de datos. Los intercambios intermediados constituyen un modelo recomendado internacionalmente tanto por la UE, como por la OCDE o la ONU, dada su demostrada eficiencia como herramienta de interoperabilidad en tanto que permite la normalización y reutilización de los servicios de intercambio.

En particular, la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos, en primer lugar y con carácter general, define los roles de los agentes que participan en los intercambios intermediados de datos; y, en segundo lugar, establece las condiciones relativas a los procesos de intercambio intermediado de datos a través de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas, condiciones asimismo aplicables a plataformas de intermediación de otras Administraciones Públicas.

Dichos roles y condiciones se establecen en términos de interoperabilidad tecnológica y se aplicarán junto a las consideraciones que correspondan a la naturaleza de la información objeto del intercambio o cesión de datos, de conformidad con la legislación que resulte de aplicación.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

## Norma Técnica de Interoperabilidad de Protocolos de Intermediación de Datos

### *I. Disposiciones generales*

I.1 Objeto.

La Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos tiene por objeto establecer las especificaciones para el intercambio intemediado de datos entre Administraciones Públicas, o Entidades de Derecho Público vinculadas o dependientes de aquellas (en adelante, organizaciones).

I.2 Ámbito de aplicación.

1. El contenido de esta norma será de aplicación para el intercambio intermediado de datos a través de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

2. Las condiciones establecidas en esta norma relativas a los agentes participantes en los intercambios intermediados de datos se aplicarán en otras plataformas de intermediación en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

3. Las condiciones establecidas en esta norma relativas a la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas podrán aplicarse en el intercambio intermediado de datos a través de otras plataformas de intermediación en el ámbito referido en el apartado 2.

4. Las condiciones establecidas en esta norma se podrán aplicar en intercambios de datos no intermediados así como en otros nodos de interoperabilidad.

*II. Agentes en los intercambios intermediados de datos*

II.1 Cedente y Emisor.

1. Un Cedente será cualquier organización que posea datos relativos a los ciudadanos que otra pueda necesitar consultar en el ámbito del ejercicio de sus competencias; es el responsable de los mismos según la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y los ofrecerá a posibles Cesionarios a través de un Emisor.

2. Un Emisor será el que facilita la cesión de los datos desde un punto de vista tecnológico.

3. Un Cedente que facilita la cesión de sus propios datos actuará, en el ámbito de esta norma, como Emisor a la vez de ser Cedente.

4. Cualquier nodo de interoperabilidad que participe en la gestión de los trámites de emisión o cesión de datos de un Emisor, tomará también el rol de Emisor en el ámbito de esta norma, incluyendo las funciones relacionadas con la firma electrónica de las comunicaciones que realiza.

5. Rol del Cedente:

a) Facilitará la información para el catálogo o registro de sus servicios de intercambio de datos disponibles bajo servicios de intercambio a disposición de otras organizaciones para su consulta.

b) Respecto a las autorizaciones de acceso a los servicios:

b.1) Establecerá los protocolos y condiciones de acceso a los servicios de intercambio de datos que ofrecen, los métodos de consulta permitidos así como la información a conocer de cada Requirente.

b.2) Justificará los casos de rechazo o denegación de una solicitud.

b.3) Definirá la política de auditoría y realizará auditorías periódicas sobre el uso del sistema relativo a las consultas de sus datos.

c) Podrá delegar estas tareas en el Emisor o en un nodo de interoperabilidad.

6. Rol del Emisor:

a) Establecerá las condiciones técnicas de acceso a los servicios de intercambio de datos que ofrece, los métodos de consulta permitidos y los controles y auditoría técnica, pudiendo delegar la ejecución de dichas condiciones en un nodo de interoperabilidad.

b) Definirá los controles y criterios de acceso a los datos necesarios para garantizar la confidencialidad de la información: políticas y procedimientos de gestión y control de acceso de usuarios y órganos.

c) Proporcionará los datos pertinentes a cada consulta con garantía de integridad y confidencialidad.

d) Informará sobre la disponibilidad de cada servicio de intercambio bajo su responsabilidad, así como sobre los mecanismos de soporte y resolución de incidencias disponibles en cada caso, incluyendo los datos de contacto para dichos servicios.

e) Definirá Acuerdos de Nivel de Servicio (ANS) para regular las condiciones de prestación de los servicios y mecanismos de respuesta a incidencias específicos acorde a la criticidad del servicio que se está prestando.

f) Mantendrá la traza de todas las peticiones recibidas y respuestas generadas.

II.2 Cesionario y Requirente.

1. Un Cesionario será cualquier organización autorizada a consultar determinados datos de los ciudadanos en poder de un Cedente.

2. Un Requirente será el que facilita la consulta de los datos desde un punto de vista tecnológico.

3. Un Cesionario que realiza directamente la consulta de datos actuará, en el ámbito de esta norma, como Requirente a la vez de ser Cesionario.

4. Cualquier nodo de interoperabilidad que participe en la gestión de los trámites de consulta de datos de un Requirente, tomará también el rol de Requirente en el ámbito de

esta norma, incluyendo las funciones relacionadas con la firma electrónica de las comunicaciones.

5. Rol del Cesionario:

a) Solicitará información siempre en relación con los trámites y procedimientos autorizados por el cedente y dentro del marco de un procedimiento administrativo.

b) Cumplirá las condiciones de acceso a los datos establecidas por el Cedente.

c) Recabará el consentimiento del interesado, salvo que una ley le exima de ello, y reflejará la respuesta obtenida del sistema, en el ámbito del expediente correspondiente.

d) Utilizará la información obtenida de cada consulta para la finalidad que corresponda en cada caso, realizando una misma consulta tantas veces como sea necesario y lo requiera el trámite a que se refiera la consulta, asumiendo expresamente la responsabilidad que pudiera derivar de posibles incumplimientos.

e) Colaborará en las labores de auditoría cuando sea requerido para ello, facilitando al Cedente la información o documentos necesarios para el control de las consultas.

6. Rol del Requirente:

a) Cumplirá las condiciones de acceso a los datos establecidas por el Emisor.

b) Asegurará que las peticiones de consulta contienen los datos de identificación, la información solicitada y la especificación del trámite o procedimiento en el que los datos serán usados y, si procede, los datos del Cesionario.

c) Mantendrá la traza de las peticiones que realiza y de las respuestas recibidas.

d) Colaborará en las labores de auditoría cuando sea requerido para ello.

e) Realizará las labores de monitorización y control necesarias para mantener un correcto funcionamiento de su servicio de consulta.

f) Asegurará las máximas garantías de seguridad y confidencialidad de las consultas, preservando la privacidad de los datos consultados tanto en el propio intercambio como en el tratamiento posterior de la información obtenida. Para ello, establecerá controles de autorización, acceso y uso por parte de los usuarios a las diferentes aplicaciones, mantendrá actualizados los datos de los usuarios y aplicaciones que acceden al sistema, notificando cualquier cambio de estado y asegurando la tramitación de su baja cuando corresponda.

g) No almacenará información personal de ningún ciudadano salvo la imprescindible para el trámite que se solicita, para la organización en nombre de la cual ha sido recabada y sólo durante el tiempo imprescindible.

*III. Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas*

III.1 Funciones.

1. El Ministerio de Hacienda y Administraciones Públicas funcionará como un nodo de interoperabilidad mediante la plataforma de Intermediación que, atendiendo a la definición de nodo de interoperabilidad recogida en el Real Decreto 4/2010, de 8 de enero, prestará funcionalidades comunes para el intercambio de información entre Emisores y Requirentes.

2. Rol de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas:

a) Gestionará los Cesionarios y Requirentes según las condiciones establecidas por cada Cedente.

b) No almacenará información personal de ningún ciudadano derivada de cualquier transacción de intercambio de datos.

c) Asegurará la confidencialidad e integridad de la información intercambiada a través de los mecanismos correspondientes.

d) Mantendrá un portal web informativo con toda la documentación relativa a la Plataforma, donde publicará al menos:

d.1) El catálogo de servicios de intercambio de datos disponibles por parte de las diferentes organizaciones, incluyendo: los protocolos de acceso a dichos servicios, los métodos de consulta permitidos, la información técnica relevante, así como la información que se requiere de cada Requirente.

d.2) Formularios de solicitud de acceso a los servicios.

d.3) Acuerdos de prestación de cada servicio disponible y de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas en general.

d.4) Novedades del servicio prestado por la Plataforma.

e) Mantendrá el sistema en funcionamiento 24x7.

f) Dará soporte a las organizaciones y gestionará todas las comunicaciones e incidencias producidas colaborando para ello con Requirentes y Emisores.

g) Mantendrá un centro de atención a usuarios e integradores que canalice todas las incidencias relativas al sistema e informará sobre los datos de contacto del mismo.

h) Elaborará informes de actividad y uso de la Plataforma considerando las consultas realizadas desde y hacia cada organización.

i) Evolucionará y mantendrá sus sistemas garantizando la seguridad y privacidad de los datos acorde a la normativa aplicable.

j) Colaborará en las labores de auditoría siempre que el Emisor o el Cedente así lo requiera y defina, conservando los datos de trazabilidad y estadísticos acordados, proporcionando acceso a los mismos cuando sea necesario y permitiendo reproducir la secuencia de operaciones llevadas a cabo por el sistema.

III.2 Gobernanza del sistema.

1. Cualquier organización podrá acceder a información sobre servicios de intercambio de datos disponibles a través de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas o, en su caso, a través del correspondiente nodo de interoperabilidad.

2. La incorporación de nuevos servicios en la Plataforma de Intermediación se coordinará entre el Ministerio de Hacienda y Administraciones Públicas y el organismo cedente correspondiente.

En el caso de servicios comunes ofrecidos por las CCAAs, la incorporación de nuevos servicios se aprobará previamente en el Comité Sectorial de Administración Electrónica.

3. Para el acceso a un servicio de intercambio de datos:

a) El Requirente enviará al Emisor la solicitud de alta para el acceso al servicio aplicando el formulario del anexo 1 a través de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas. Esta operación se realizará para cada Cesionario que gestione el Requirente.

b) El Emisor remitirá al Requirente la autorización del cesionario en respuesta a dicha solicitud. Dicha autorización contemplará la justificación de la legitimidad y competencia del Requirente y será registrada por la Plataforma de intermediación.

4. Las funciones de cada agente involucrado en la autorización podrán ser realizadas por la propia Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas o, en su caso, por un nodo de interoperabilidad que haya subscrito el correspondiente convenio con este Ministerio a tal efecto.

III.3 Requisitos técnicos.

1. La Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas garantizará la interoperabilidad, disponibilidad, fiabilidad y seguridad de la información transmitida a través de ella entre las diferentes organizaciones con las que interactúa.

2. En el acceso a la Plataforma de intermediación de datos del Ministerio de Hacienda y Administraciones Públicas se utilizará la Red de comunicaciones de las Administraciones públicas españolas atendiendo a lo establecido en la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas.

III.4 Aspectos generales de seguridad.

El intercambio de datos entre la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas y las organizaciones se realizará en unas condiciones tales que garanticen la seguridad de la información que se transmite, proporcionando medidas para la

autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad adecuadas a la naturaleza de la misma:

a) Autenticidad. Se asegurará la identidad de todos los agentes que intervengan en el proceso de intercambio de datos, de forma que todos ellos estén correctamente identificados en cada intercambio. Para ello, se aplicarán las medidas de seguridad contempladas en el Real Decreto 3/2010, de 8 de enero, dentro del grupo «marco operacional» en el capítulo relativo a «Control de acceso» (op.acc); y del grupo «medidas de protección», en el capítulo «Protección de la información» (mp.info).

b) Confidencialidad e integridad de la información intercambiada, que será protegida conforme al grupo de «medidas de protección», capítulos «Protección de las comunicaciones» (mp.com) y «Protección de la información» (mp.info) definidas en el Real Decreto 3/2010, de 8 de enero, y con las medidas de seguridad dispuestas en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, asegurando que no se almacena información personal de ningún ciudadano.

c) Disponibilidad de la Plataforma, asegurada a través de medidas establecidas en el capítulo «Protección de los servicios» (mp.$) del grupo de «medidas de protección» definidas en el Real Decreto 3/2010, de 8 de enero.

d) Trazabilidad, según lo establecido en el apartado 111.6 de esta norma.

III.5 Tecnologías y estándares.

1. Las tecnologías utilizadas para los intercambios se implementarán en base a estándares abiertos e interoperables según lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares.

2. Los intercambios de información se podrán implementar a través de servicios web, que, como conjunto de protocolos y estándares abiertos sobre los que desarrollar estructuras de datos específicas para cada tipo de intercambio, incorporarán los mecanismos de seguridad necesarios para la comunicación.

3. Los servicios web implementados se diseñarán en base a la utilización de:

a) Servicios definidos mediante un lenguaje WSDL *(Web Services Description Language).*

b) Mensajes en formato XML (eXtensible Mark-up Language) con estructuras basadas en esquemas XML publicados que faciliten su interpretación.

c) Estándares de seguridad en las comunicaciones a nivel de transporte punto a punto, mediante el uso del protocolo TLS *(Transport Layer Security)* con autenticación de cliente a nivel de transporte, o a nivel de aplicación mediante el uso de protocolos que garanticen la seguridad extremo a extremo en servicios Web.

4. De forma general en servicios de intercambio se utilizará la versión 3.0 del protocolo SCSP (Sustitución de Certificados en Soporte Papel) cuya especificación está disponible en el Portal de Administración electrónica PAE/CTT en la dirección http://administracionelectronica.gob.es/es/ett/sesp.

Se podrá utilizar la versión 2 del protocolo SCSP en servicios ya existentes que no requieran mecanismos adicionales de seguridad sin perjuicio de que exista una versión actualizada del mismo servicio.

III.6 Trazabilidad y auditoría de los intercambios.

1. Emisores y Requirentes mantendrán trazabilidad de los intercambios de datos producidos, para lo cual podrán apoyarse en funcionalidades prestadas por la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas, y en lo previsto sobre trazabilidad en el Real Decreto 3/2010, de 8 de enero.

2. La conservación de trazas por parte de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas, establecida atendiendo a las medidas de seguridad contempladas en el Real Decreto 3/2010, de 8 de enero: op.exp.10 «Protección de los registros de actividad», op.exp.8 «Registro de la actividad de los usuarios», mp.info.5 «Sellos de tiempo», facilitará la auditoría de los intercambios. La información aportada por la Plataforma se completará con aquella que permita la recuperación de los datos específicos intercambiados que conservarán Emisor y Requirente.

3. La Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas no almacenará información sobre el contenido del intercambio ni asumirá funciones relativas a la conservación de trazas y auditoría, mas allá de lo establecido en el apartado 111.6 y en cuyo caso la definición de funciones y mecanismos de puesta a disposición del agente interesado será documentada convenientemente. El Cedente podrá auditar la cesión de datos para comprobar el cumplimiento de los requisitos a que pudiera ésta estar sujeta.

4. Para garantizar la trazabilidad de los intercambios producidos, se asociará a cada petición o consulta un identificador único que permitirá reproducir la secuencia de operaciones llevadas a cabo.

5. La información almacenada para la trazabilidad de cada consulta o intercambio contemplará, al menos, lo siguiente:

a) Identificador de la transacción.

b) Cesionario de la información, Requirente que la solicita y usuario final que la realiza especificando, si es posible, el empleado público o aplicación.

c) Tipo de información que se solicita.

d) Fecha y hora de realización de la consulta.

III.7 Catálogo de servicios de intercambio de datos.

1. El catálogo o registro de los servicios de intercambio de datos ofrecidos por cada Cedente será incorporado al catálogo de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas sirviendo de referencia a posibles Requirentes.

2. El catálogo de servicios de intercambio de datos estará disponible para su consulta por las distintas organizaciones a través de alguno de los siguientes medios:

a) Un punto informativo propio del Cedente o del Emisor, si se delega en éste por parte del Cedente, que podrá ser su sede electrónica.

b) La Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas.

c) Los instrumentos para la interoperabilidad establecidos en el Real Decreto 4/2010, de 8 de enero:

i. Inventario de procedimientos administrativos y servicios prestados.

ii. Centro de Interoperabilidad Semántica de la Administración.

3. En el catálogo o registro de servicios figurará, para cada servicio disponible o supuesto genérico de intercambio, al menos, la información general definida en el anexo 11.

4. Para la publicación de nuevos servicios en la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas se podrá utilizar UDDI (Universal Description, Discovery and Integration) o un servicio de directorio como medio para facilitar el descubrimiento dinámico de nuevos servicios, aunque el uso de aquellos dependerá en cualquier caso de la formalización de las autorizaciones necesarias correspondientes.

# § 19

## Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Relación de modelos de datos

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 178, de 26 de julio de 2012
Última modificación: sin modificaciones
Referencia: BOE-A-2012-10050

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, la norma relativa a la publicación de modelos de datos responde a lo previsto en el artículo 10 del citado Real Decreto 4/2010, de 8 de enero, sobre activos semánticos.

En particular, la Norma Técnica de Interoperabilidad de Relación de modelos de datos define las condiciones para establecer y publicar los modelos de datos a los que se refiere el citado artículo 10 relativas al formato, identificación y documentación asociada a los modelos de datos, a sus posibles usos así como a sus definiciones y codificaciones asociadas, al objeto de facilitar la interacción con el Centro de Interoperabilidad Semántica, encargado de su publicación. Este modelo de intercambio y publicación de modelos de datos está alineado

con prácticas y estándares reconocidos a nivel europeo promovidos desde SEMIC.EU: Semantic Interoperability Centre Europe.

En cuanto a las definiciones y codificaciones asociadas a los modelos de datos, atendiendo al epígrafe cuatro del citado artículo 10, la norma establece las condiciones para que, aquellas de interés estadístico, tengan en cuenta los modelos estándares establecidos por el Instituto Nacional de Estadística con el fin de asegurar la aplicación de sistemas normalizados de conceptos, definiciones, unidades estadísticas, clasificaciones, nomenclaturas y códigos que hagan factible la comparación, la integración y el análisis de los datos y los resultados obtenidos, tal y como establece la Ley 12/1989, de 9 de mayo, de la Función estadística pública. Por otra parte, la norma establece el uso de la codificación de Unidades Orgánicas y Oficinas de la Administración a través del Directorio Común gestionado por el Ministerio de Hacienda y Administraciones Públicas para la descripción de los modelos de datos.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Relación de modelos de datos cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Relación de modelos de datos que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la Disposición Transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

## NORMA TÉCNICA DE INTEROPERABILIDAD DE RELACIÓN DE MODELOS DE DATOS

### *I. Objeto*

La Norma Técnica de Interoperabilidad de Relación de modelos de datos tiene por objeto definir las condiciones para establecer y publicar modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras administraciones, así como las definiciones y codificaciones asociadas, de cara a su publicación en el Centro de Interoperabilidad Semántica.

### *II. Ámbito de aplicación*

El contenido de esta norma será de aplicación en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

### *III. Modelos de datos a publicar*

Los órganos de la Administración pública y las Entidades de Derecho Público vinculadas o dependientes de aquélla establecerán y compartirán, junto a las definiciones y codificaciones asociadas, los modelos de datos de los que sean titulares y se refieran a:

a) Materias sujetas a intercambio de información con los ciudadanos y con otras Administraciones públicas.

b) Infraestructuras, servicios y herramientas comunes, que no sean de uso exclusivamente interno a la organización.

*IV. Estructura de intercambio de los modelos de datos*

Los modelos de datos a publicar en el Centro de Interoperabilidad Semántica (CISE) se ajustarán a la estructura de intercambio definida en el anexo I conteniendo:

a) Activos semánticos, en formato XSD (XML Schema Definition), clasificados según los servicios ó unidades de negocio de las diferentes administraciones.

b) Guías explicativas, en formato PDF (Portable Document Format), atendiendo a lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares, de los diferentes servicios ó sistemas de intercambio, que incluirán:

i. Descripción de los tipos y definiciones de datos que se intercambian bajo el modelo de datos de que se trate, así como una descripción funcional de las operaciones que se pueden realizar.

ii. Breve descripción de las condiciones de seguridad aplicables a los intercambios con dicho modelo.

iii. Condiciones que deben cumplir lo receptores de la información a la que aplica el modelo en cuestión.

iv. Ejemplos de implementación de los diferentes servicios bajo el modelo de datos que corresponda.

v. De forma opcional, manuales de ayuda del servicio de intercambio y juegos de pruebas.

*V. Identificación de los modelos de datos*

V.1 Los órganos de la Administración pública o Entidades de Derecho Público vinculadas o dependientes de aquélla proporcionarán una identificación de la estructura de intercambio de sus modelos de datos, que permitirá su clasificación y facilitará al Centro de Interoperabilidad Semántica las tareas de identificación, localización y clasificación de los modelos de datos cuya publicación centraliza.

V.2 La información para la identificación de los modelos de datos incluirá, al menos, los datos descritos en el anexo II.

V.3 La descripción de los modelos de datos se ajustará a los estándares establecidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares.

V.4 Para darse de alta en el Centro de Interoperabilidad Semántica, el órgano responsable de los modelos de datos remitirá un mensaje por correo electrónico a la dirección « admin.cise@seap.minhap.es», que antepondrá como asunto del mismo el encabezamiento «ALTA CISE» + «Identificador Normalizado de órgano extraído del Directorio Común de Organismos y Oficinas gestionado por el MINHAP» y contendrá en el cuerpo del mensaje la siguiente información: «Nombre del organismo emisor», «Dirección URL», «Dirección de correo electrónico».

*VI. Interacción con el Centro de Interoperabilidad Semántica*

Para su interacción con el Centro de Interoperabilidad Semántica, cada órgano de la Administración pública o Entidad de Derecho Público vinculada o dependiente de aquélla:

a) Identificará los modelos de datos susceptibles de ser intercambiados con el Centro de Interoperabilidad Semántica, atendiendo a lo establecido en el apartado V de la presente norma técnica.

b) Facilitará la estructura de intercambio de los modelos de datos al Centro de Interoperabilidad Semántica mediante uno de los siguientes procedimientos, asegurando en cualquier caso la actualización de la información facilitada:

i. Recopilación y depósito de los modelos de datos, estructurados según el apartado IV, en un entorno de intercambio accesible por el Centro de Interoperabilidad Semántica a

través de la Red de comunicaciones de las Administraciones públicas españolas, para su carga masiva.

Dicho entorno será convenientemente identificado a través de la correspondiente URL (Uniform Resource Locator) definida por el propietario del modelo de datos y que atenderá a lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares.

ii. Publicación de cada modelo de datos directamente a través de las herramientas que disponga el Centro de Interoperabilidad Semántica y atendiendo al procedimiento de utilización que éste establezca.

c) Actualizará de manera proactiva la información facilitada al Centro de Interoperabilidad Semántica, bien a través del entorno de intercambio o a través de las herramientas que el Centro de Interoperabilidad Semántica establezca a tal efecto.

d) Podrá consultar los modelos de datos disponibles en el repositorio de información del Centro de Interoperabilidad Semántica y recibir notificaciones automáticas de dicho Centro ante la publicación y actualización de modelos de datos.

*VII. Uso de los modelos de datos*

VII.1 Los modelos de datos comunes publicados en el Centro de Interoperabilidad Semántica serán de preferente aplicación según lo establecido en el artículo 10.1 del Real Decreto 4/2010, de 8 de enero.

VII.2 Los modelos de datos de titulares de competencias en materias sujetas a intercambio de información con los ciudadanos y con otras Administraciones públicas, así como en materia de infraestructuras, servicios y herramientas comunes publicados en el Centro de Interoperabilidad Semántica serán de obligatoria aplicación según lo establecido en el artículo 10.2 del Real Decreto 4/2010, de 8 de enero.

VII.3 El Centro de Interoperabilidad Semántica identificará convenientemente los modelos de datos comunes de obligatoria aplicación, diferenciándolos de otros modelos de datos aportados por las diferentes administraciones.

VII.4 En el Comité Sectorial de Administración Electrónica se identificarán, catalogarán y priorizarán los modelos de datos comunes.

*VIII. Codificaciones*

VIII.1 Las definiciones y codificaciones de interés estadístico:

a) Serán aquellas que dispongan de un modelo estándar definido por el Instituto Nacional de Estadística disponible en el portal del Instituto y en el Centro de Interoperabilidad Semántica.

b) Serán identificadas en los modelos de datos de las que formen parte según lo dispuesto en el apartado V de esta norma.

c) Ante su presencia en nuevos modelos o en actualizaciones de modelos de datos existentes publicados en el Centro de Interoperabilidad Semántica, podrán ser contrastadas por el Instituto Nacional de Estadística con sus modelos estándar.

En caso de que dichos modelos de datos no se ajusten a los modelos estándar definidos, el Instituto Nacional de Estadística lo pondrá en conocimiento del Ministerio de Hacienda y Administraciones Públicas, quien lo pondrá en conocimiento de la Administración o Entidad responsable a los efectos oportunos.

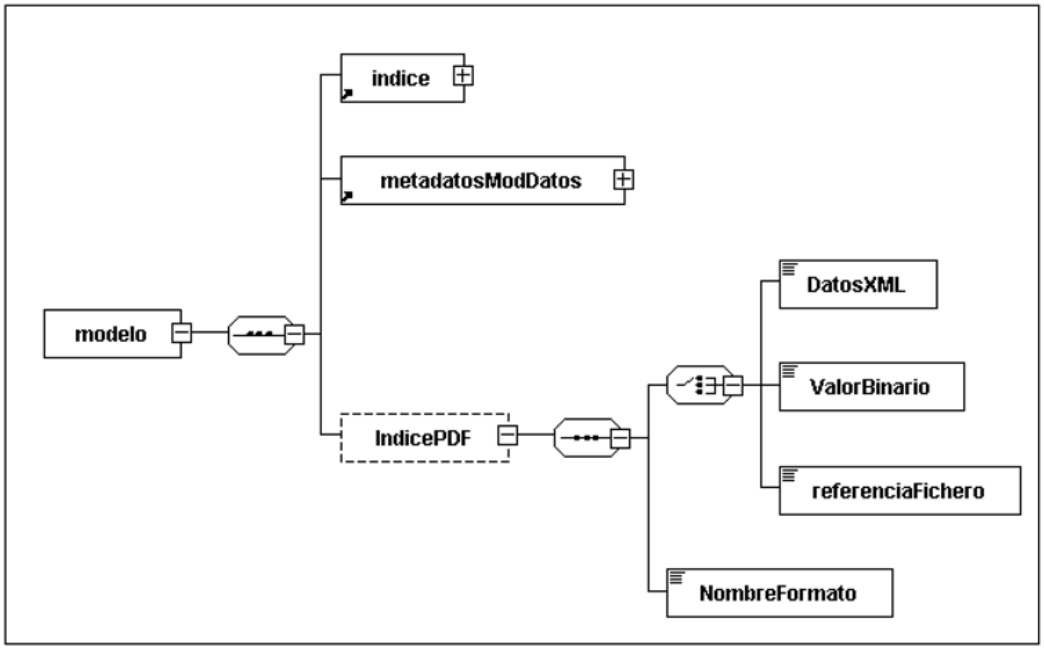
VIII.2 La codificación de Unidades Orgánicas y Oficinas de la Administración en los modelos de datos aplicará las establecidas en el Directorio Común de Organismos y Oficinas, que será gestionado por el Ministerio de Hacienda y Administraciones Públicas y alimentado por todos los órganos de la Administración pública o Entidades de Derecho Público vinculadas o dependientes de aquélla.

El Centro de Interoperabilidad Semántica publicará toda la documentación de integración, procedimientos de colaboración, y definición de atributos de la información del Directorio, teniendo en cuenta lo recogido en esta norma sobre intercambio de modelos de datos. Asimismo, dicho Centro publicará y mantendrá actualizada una relación de las fuentes colaboradoras y un enlace a la aplicación de gestión del Directorio Común.

## ANEXO I

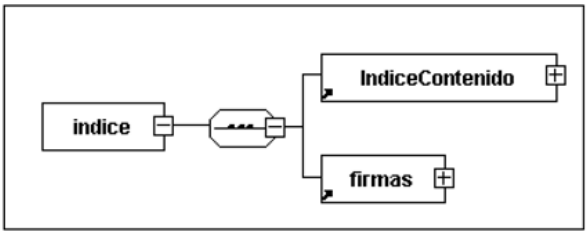
## Esquemas XML para publicación de modelos de datos

1. *XSD Modelo de datos*



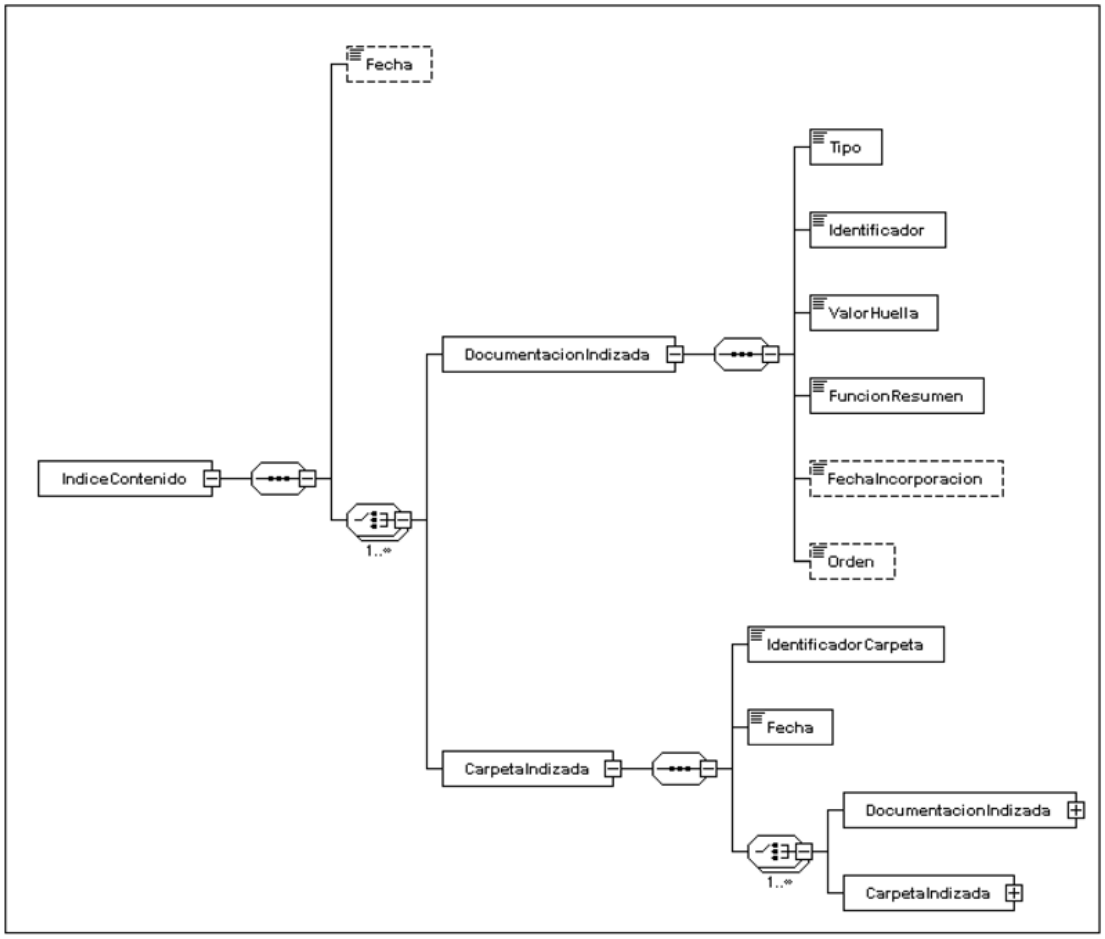

```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ModDatosInd="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice"
xmlns:ModDatosMeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/metadatos"
xmlns:ModDatos="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos"
xmlns:enifile="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD MODELOS DE DATOS versión 1.0 - 25/10/2011.</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice" schemaLocation="
http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/IndiceModDatos.xsd" />
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/metadatos" schemaLocation="
http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/metadatos/MetadatosModDatos.xsd" />
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido" schemaLocation="
http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido/contenidoDocumentoEni.xsd" />
<xsd:element name="modelo" type="ModDatos:TipoModelo" />

<xsd:complexType name="TipoModelo">
        <xsd:sequence>
                <xsd:element ref="ModDatosInd:indice" />
                <xsd:element ref="ModDatosMeta:metadatosModDatos" />
                <xsd:element name="IndicePDF" type="enifile:TipoContenido" minOccurs="0" />
        </xsd:sequence>
         <xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>
</xsd:schema>
```

2. *XSD Índice del modelo de datos*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma"
xmlns:ModDatosInd="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice"
xmlns:ModDatosIndcon="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD INDICE MODELO DE DATOS versión 1.0 - 25/10/2011.</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma" schemaLocation="
http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma/firmasEni.xsd" />
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/contenido" schemaLocation="
http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/contenido/IndiceModDatosCon.xsd" />
<xsd:element name="indice" type="ModDatosInd:TipoIndice" />

<xsd:complexType name="TipoIndice">
        <xsd:sequence>
                <xsd:element ref="ModDatosIndcon:IndiceContenido" />
                <xsd:element ref="enids:firmas" />
        </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>

</xsd:schema>
```

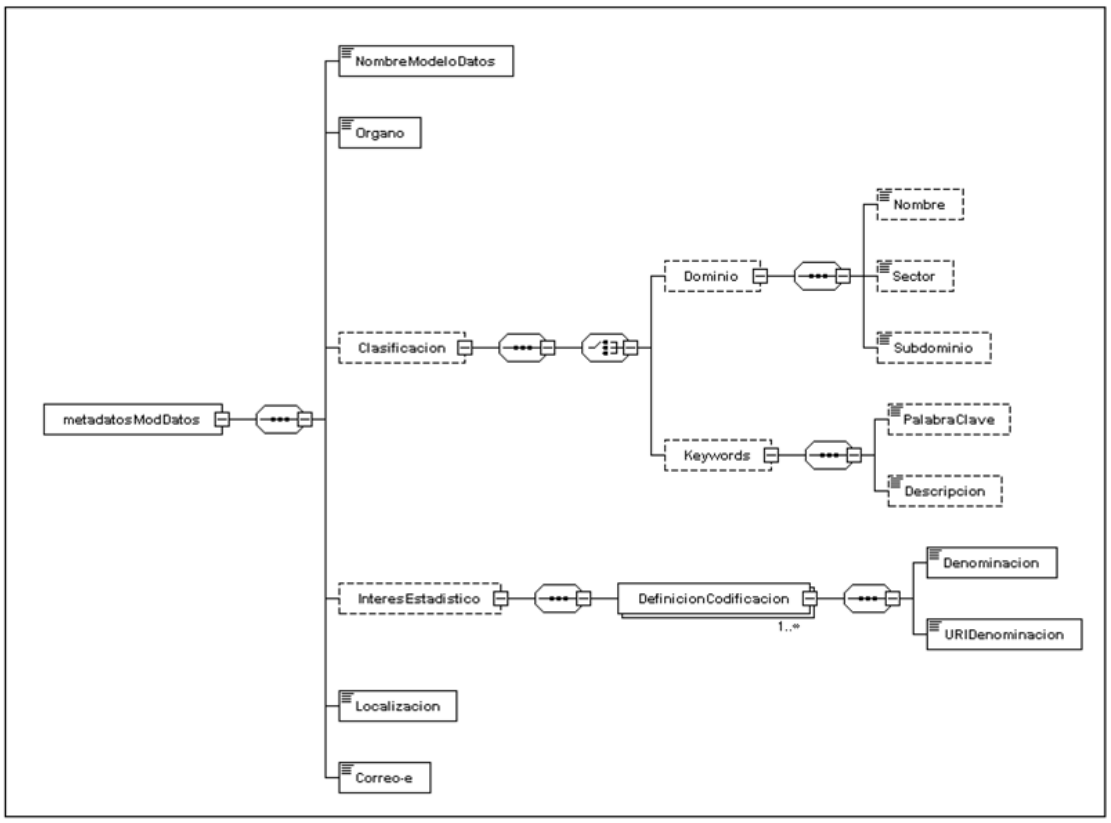
3. *XSD Contenido del índice del modelo de datos*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ModDatosIndcon="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/contenido" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD CONTENIDO INDICE MODELO DE DATOS version 1.0 -
        25/10/2011.</xsd:documentation>
</xsd:annotation>
```

```
<xsd:element name="IndiceContenido" type="ModDatosIndcon:TipoIndiceContenido" />
<xsd:complexType name="TipoIndiceContenido">
	<xsd:sequence>
		<xsd:element name="Fecha" type="xsd:dateTime" minOccurs="0" />
		<xsd:choice maxOccurs="unbounded">
			<xsd:element name="DocumentacionIndizada" type="ModDatosIndcon:TipoIndizado" />
			<xsd:element name="CarpetaIndizada" type="ModDatosIndcon:TipoCarpetaIndizada" />
		</xsd:choice>
	</xsd:sequence>
	<xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>

<xsd:complexType name="TipoIndizado">
	<xsd:sequence>
		<xsd:element name="Tipo" type="xsd:boolean">
			<xsd:annotation>
				<xsd:documentation xml:lang="es">0-Documentacion complementaria. 1-Modelo de datos
				(XSD).</xsd:documentation>
			</xsd:annotation>
		</xsd:element>
		<xsd:element name="Identificador" type="xsd:string" />
		<xsd:element name="ValorHuella" type="xsd:string" />
		<xsd:element name="FuncionResumen" type="xsd:string" />
		<xsd:element name="FechaIncorporacion" type="xsd:dateTime" minOccurs="0" />
		<xsd:element name="Orden" type="xsd:string" minOccurs="0" />
	</xsd:sequence>
	<xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>

<xsd:complexType name="TipoCarpetaIndizada">
	<xsd:sequence>
		<xsd:element name="IdentificadorCarpeta" type="xsd:string" />
		<xsd:element name="Fecha" type="xsd:dateTime" />
		<xsd:choice maxOccurs="unbounded">
			<xsd:element name="DocumentacionIndizada" type="ModDatosIndcon:TipoIndizado" />
			<xsd:element name="CarpetaIndizada" type="ModDatosIndcon:TipoCarpetaIndizada" />
		</xsd:choice>
	</xsd:sequence>
	<xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>
</xsd:schema>
```

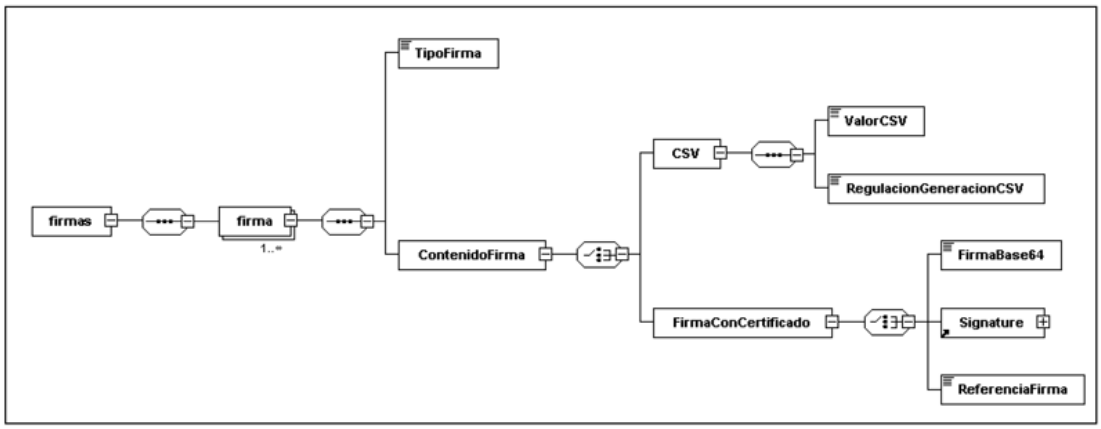
4. *XSD Metadatos del modelo de datos*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ModDatosMeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/metadatos"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/metadatos" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD METADATOS MODELOS DE DATOS versión 1.0 -
        25/10/2011.</xsd:documentation>
</xsd:annotation>
```

```
<xsd:element name="metadatosModDatos" type="ModDatosMeta:TipoMetadatos" />

<xsd:complexType name="TipoMetadatos">
        <xsd:sequence>
                <xsd:element name="NombreModeloDatos" type="xsd:string" />
                <xsd:element name="Organo" type="xsd:string" >
                        <xsd:annotation>
                                <xsd:documentation xml:lang="es"> Código alfanumérico único para cada órgano/unidad/oficina
                                extraído del Directorio Común gestionado por el Ministerio de Hacienda y Administraciones
                                Públicas.</xsd:documentation>
                        </xsd:annotation>
                </xsd:element >
                <xsd:element name="Clasificacion" type="ModDatosMeta:TipoClasificacion" minOccurs="0" />
                <xsd:element name="InteresEstadistico" type="ModDatosMeta:TipoInteresEstadistico" minOccurs="0"
                maxOccurs="1">
                        <xsd:annotation>
                                <xsd:documentation xml:lang="es"> Identificación unívoca de la definición y codificación de
                                interés estadístico del modelo de datos definida por el Instituto Nacional de
                                Estadística.</xsd:documentation>
                        </xsd:annotation>
                </xsd:element >
                <xsd:element name="Localizacion" type="xsd:anyURI" />
                 <xsd:element name="Correo-e" type="xsd:string" />
         </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>

<xsd:complexType name="TipoClasificacion">
        <xsd:sequence>
                <xsd:choice>
                        <xsd:element name="Dominio" type="ModDatosMeta:TipoDominio" minOccurs="0" />
                        <xsd:element name="Keywords" type="ModDatosMeta:TipoKeywords" minOccurs="0" />
                </xsd:choice>
        </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="TipoDominio">
        <xsd:sequence>
                <xsd:element name="Nombre" type="xsd:string" minOccurs="0" />
                <xsd:element name="Sector" type="xsd:string" minOccurs="0" />
                <xsd:element name="Subdominio" type="xsd:string" minOccurs="0" />
        </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="TipoKeywords">
        <xsd:sequence>
                <xsd:element name="PalabraClave" type="xsd:string" minOccurs="0" />
                <xsd:element name="Descripcion" type="xsd:string" minOccurs="0" />
        </xsd:sequence>
 </xsd:complexType>

<xsd:complexType name="TipoInteresEstadistico">
        <xsd:sequence>
                <xsd:element name="DefinicionCodificacion" type="ModDatosMeta:TipoDefinicionCodificacion" minOccurs="1"
                maxOccurs="unbounded" />
         </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="TipoDefinicionCodificacion">
        <xsd:sequence>
                <xsd:element name="Denominacion" type="xsd:string" />
                <xsd:element name="URIDenominacion" type="xsd:anyURI" />
        </xsd:sequence>
 </xsd:complexType>
 </xsd:schema>
```

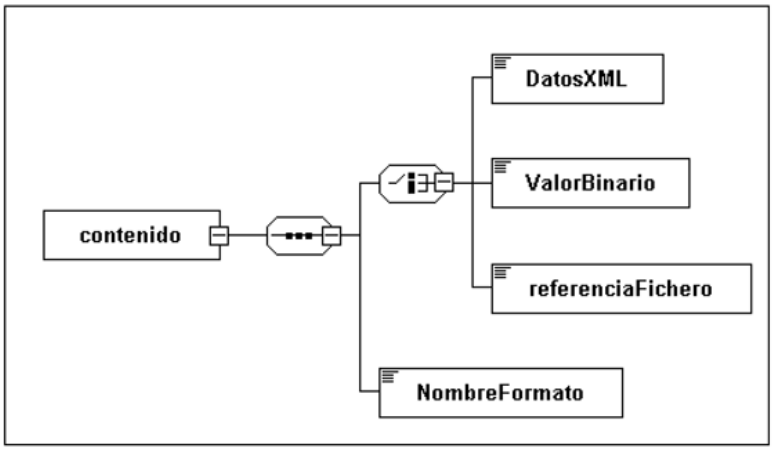
5. *XSD Firmas*




```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma " xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma " elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD FIRMAS ELECTRONICAS ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-
schema.xsd"/>
<xsd:element name="firmas" type="enids:firmas"/>
<xsd:complexType name="firmas">
        <xsd:sequence>
                <xsd:element name="firma" type="enids:TipoFirmasElectronicas" minOccurs="1" maxOccurs="unbounded"/>
        </xsd:sequence>
</xsd:complexType>
```

```
<xsd:complexType name="TipoFirmasElectronicas">
	<xsd:sequence>
		<xsd:element name="TipoFirma">
			<xsd:annotation>
				<xsd:documentation xml:lang="es">
					- TF01 - CSV.
					- TF02 - XAdES internally detached signature.
					- TF03 - XAdES enveloped signature.
					- TF04 - CAdES detached/explicit signature.
					- TF05 - CAdES attached/implicit signature.
					- TF06 - PAdES.
				</xsd:documentation>
			</xsd:annotation>
			<xsd:simpleType>
				<xsd:restriction base="xsd:string">
					<xsd:enumeration value="TF01"/>
					<xsd:enumeration value="TF02"/>
					<xsd:enumeration value="TF03"/>
					<xsd:enumeration value="TF04"/>
					<xsd:enumeration value="TF05"/>
					<xsd:enumeration value="TF06"/>
				</xsd:restriction>
			</xsd:simpleType>
		</xsd:element>
		<xsd:element name="ContenidoFirma">
			<xsd:complexType>
				<xsd:choice>
					<xsd:element name="CSV">
						<xsd:complexType>
							<xsd:sequence>
								<xsd:element name="ValorCSV" type="xsd:string"/>
								<xsd:element name="RegulacionGeneracionCSV"
								type="xsd:string"/>
							</xsd:sequence>
						</xsd:complexType>
					</xsd:element>
					<xsd:element name="FirmaConCertificado">
						<xsd:complexType>
							<xsd:choice>
								<xsd:element name="FirmaBase64"
								type="xsd:base64Binary"/>
								<xsd:element ref="ds:Signature"/>
								<xsd:element name="ReferenciaFirma">
									<xsd:annotation>
									<xsd:documentation  xml:lang="es">
									Referencia interna al fichero que incluye la firma.
									</xsd:documentation>
									</xsd:annotation>
								</xsd:element>
							</xsd:choice>
						</xsd:complexType>
					</xsd:element>
				</xsd:choice>
			</xsd:complexType>
		</xsd:element>
	</xsd:sequence>
<xsd:attribute name="Id" type="xsd:ID" use="optional"/>
<xsd:attribute name="ref" type="xsd:string" use="optional">
	<xsd:annotation>
		<xsd:documentation xml:lang="es">Almacena el identificador del nodo que se está firmando. En caso de firmas
		multinodo, se incluirá una lista separada por comas de los identificadores de los nodos firmados.
		</xsd:documentation>
	</xsd:annotation>
</xsd:attribute>
</xsd:complexType>
</xsd:schema>
```

6. *XSD Contenido de Documento electrónico*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:enifile="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD CONTENIDO DOCUMENTO ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:element name="contenido" type="enifile:TipoContenido"/>
<xsd:complexType name="TipoContenido">
        <xsd:sequence>
                <xsd:choice>
                        <xsd:element name="DatosXML" type="xsd:anyType">
                                <xsd:annotation>
                                        <xsd:documentation xml:lang="es">Contenido en formato XML. En caso de datos XML
                                        cuya codificación difiera de la de esta estructura raiz se incluirá una cláusula
                                        CDATA.</xsd:documentation>
                                </xsd:annotation>
                        </xsd:element>
                        <xsd:element name="ValorBinario" type="xsd:base64Binary">
                                <xsd:annotation>
                                        <xsd:documentation xml:lang="es">Contenido en base64.</xsd:documentation>
                                </xsd:annotation>
                        </xsd:element>
                        <xsd:element name="referenciaFichero" type="xsd:string">
                                <xsd:annotation>
                                        <xsd:documentation xml:lang="es">Referencia interna al fichero de contenido.
                                        </xsd:documentation>
                                </xsd:annotation>
                        </xsd:element>
                </xsd:choice>
                <xsd:element name="NombreFormato" type="xsd:string">
                        <xsd:annotation>
                                <xsd:documentation xml:lang="es">El formato del fichero de contenido del documento
                                electrónico atenderá a lo establecido en la NTI de Catálogo de estándares.
                                </xsd:documentation>
                        </xsd:annotation>
                </xsd:element>
        </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

## ANEXO II

## Identificación de los modelos de datos

*Tabla 1. Identificación de los modelos de datos*

| Información | Descripción |
|---|---|
| Nombre | Nombre identificativo del modelo de datos. |
| Órgano | Identificador normalizado del órgano o entidad de la Administración que pone a disposición el activo, extraído del Directorio Común gestionado por el MINHAP. |

| Información | Descripción |
|---|---|
| Interés estadístico | Denominación de las definiciones y codificaciones de interés estadístico contenidas en el modelo. |
| Localización | Localización del servicio de intercambio tipo URI (Uniform Resource Identifier). En caso de estar disponible, localización del Servicio web correspondiente. |
| Correo-e de la unidad generadora | Correo electrónico de la unidad generadora de los modelos de datos, necesario para gestión en la comunicación con el Centro de Interoperabilidad Semántica. |

# § 20

## Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 178, de 26 de julio de 2012
Última modificación: sin modificaciones
Referencia: BOE-A-2012-10048

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: Documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

En particular, la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos establece los conceptos relacionados con el desarrollo de políticas de gestión de documentos electrónicos, identifica los procesos de la gestión de documentos en el marco de la administración electrónica y establece los principios necesarios para el desarrollo y aplicación de políticas de gestión de documentos electrónicos por parte de todos los órganos de la Administración y Entidades de Derecho Público vinculadas o dependientes de aquélla.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la Disposición Transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

## Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos

### *I. Objeto*

La Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos tiene por objeto establecer las directrices para la definición de políticas de gestión de documentos electrónicos.

### *II. Ámbito de aplicación*

II.1 El contenido de esta norma será de aplicación para el desarrollo de políticas de gestión de documentos electrónicos en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

II.2 Las directrices establecidas en esta norma se podrán aplicar en el desarrollo de políticas de gestión de documentos en entornos híbridos en que convivan documentos en soporte papel y documentos electrónicos.

### *III. Contenido y contexto*

III.1 La política de gestión de documentos electrónicos será un documento que incluirá:

1. Definición del alcance y ámbito de aplicación.
2. Roles de los actores involucrados.
3. Directrices para la estructuración y desarrollo de los procedimientos de gestión documental.
4. Acciones de formación relacionada contempladas.
5. Actuaciones de supervisión y auditoría de los procesos de gestión de documentos.

6. Proceso de revisión del contenido de la política con el fin de garantizar su adecuación a la evolución de las necesidades de la gestión de documentos.

III.2 La política de gestión de documentos electrónicos:

1. Se integrará en el marco general de gestión de documentos y en el contexto de cada organización junto al resto de políticas implantadas para el desempeño de sus actividades.
2. Aplicará los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como los estándares y buenas prácticas nacionales e internacionales aplicables para la gestión documental atendiendo a lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares.

*IV. Actores involucrados*

Los actores involucrados en la definición, aprobación e implantación de la política de gestión de documentos electrónicos en una organización, serán, al menos, los siguientes:

1. La alta dirección que aprobará e impulsará la política.
2. Los responsables de procesos de gestión que aplicarán la política en el marco de los procesos de gestión a su cargo.
3. El personal responsable de la planificación, implantación y administración del programa de tratamiento de documentos y sus operaciones, cualificado, dedicado e instruido en gestión y conservación documental y que participará en el diseño, implementación y actualización de los sistemas de gestión y conservación documental.
4. El personal implicado en tareas de gestión de documentos electrónicos que aplicará lo establecido en la política a través del programa de tratamiento implantado.

*V. Programa de tratamiento de documentos electrónicos*

V.1 El diseño, desarrollo e implantación de los procesos, técnicas y operaciones de gestión de documentos electrónicos se concretará en un programa de tratamiento específico para la gestión de documentos y expedientes electrónicos.
V.2 Dicho programa de tratamiento se aplicará de manera continua sobre todas las etapas o periodos del ciclo de vida de los documentos y expedientes electrónicos para los que garantizará su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad; permitiendo la protección, recuperación y conservación física y lógica de los documentos y su contexto.

*VI. Procesos de gestión de documentos electrónicos*

Los procesos de gestión de documentos electrónicos de una organización incluirán, al menos, los siguientes:

1. Captura de documentos, que incluirá el tratamiento de los metadatos mínimos obligatorios definidos en la Norma Técnica de Interoperabilidad de Documento Electrónico.
2. Registro legal de documentos, definido en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común que, además del tratamiento de documentos electrónicos recibidos, atenderá a la posibilidad de digitalizar documentos en soporte papel según lo establecido en la Norma Técnica de Interoperabilidad de Digitalización de Documentos.
3. Clasificación de documentos, que incluirá los criterios de formación de expedientes y agrupaciones de documentos electrónicos según la Norma Técnica de Interoperabilidad de Expediente Electrónico, así como la clasificación funcional de acuerdo con el cuadro de clasificación de la organización.
4. Descripción de documentos, que atenderá a lo establecido en el apartado VII de esta norma así como a la posible redacción de un esquema institucional de metadatos.
5. Acceso a los documentos, que contemplará la posible regulación institucional de dicha práctica así como la trazabilidad de las acciones que se realizan sobre cada uno de ellos.
6. Calificación de los documentos, que incluirá:

i. Determinación de los documentos esenciales.

ii. Valoración de documentos y determinación de plazos de conservación.
iii. Dictamen de la autoridad calificadora.

7. Conservación de los documentos en función de su valor y tipo de dictamen de la autoridad calificadora, a través de la definición de calendarios de conservación.

8. Transferencia de documentos, que incluirá las consideraciones para la transferencia entre repositorios así como las responsabilidades en cuanto a su custodia.

9. Destrucción o eliminación de los documentos, que atenderá a la normativa aplicable en materia de eliminación de Patrimonio Documental y contemplará la aplicación de las medidas de seguridad relacionadas definidas en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica: Borrado y destrucción del capítulo de «Protección de los soportes de información [mp.si]» y Limpieza de documentos del capítulo de «Protección de la información [mp.info]».

*VII. Asignación de metadatos*

VII.1 Las organizaciones garantizarán la disponibilidad e integridad de los metadatos de sus documentos electrónicos, manteniendo de manera permanente las relaciones entre cada documento y sus metadatos.

VII.2 La implementación de los metadatos de gestión de documentos electrónicos para su tratamiento y gestión a nivel interno será diseñada por cada organización en base a sus necesidades, criterios y normativa específica.

VII.3 Los metadatos de gestión de documentos electrónicos se articularán en esquemas de metadatos que responderán a las particularidades y necesidades específicas de gestión de cada organización.

VII.4 El Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE), disponible en el Centro de Interoperabilidad Semántica, que incluye los metadatos mínimos obligatorios, definidos en las Normas Técnicas de Interoperabilidad de Documento electrónico y Expediente electrónico, así como otros metadatos complementarios pertinentes en una política de gestión y conservación de documentos electrónicos, podrá ser utilizado como referencia para la adecuación a los requisitos de interoperabilidad en materia de gestión documental.

*VIII. Documentación*

Cada organización elaborará y mantendrá actualizados y documentados los procedimientos de gestión de documentos a seguir en los distintos procesos de gestión documental.

*IX. Formación*

IX.1 El personal de las organizaciones recibirá la formación específica y adecuada a su rol necesaria para la gestión y conservación de documentos y expedientes electrónicos.

IX.2 Las organizaciones exigirán, de manera objetiva y no discriminatoria, que aquellos que les presten servicios relacionados con la gestión y conservación documental cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

*X. Supervisión y auditoría*

X.1 Los procedimientos y acciones seguidos en los distintos procesos de gestión documental generarán registros con las evidencias de la correcta aplicación de dichos procedimientos atendiendo a las necesidades de cada documento y organización.

X.2 Las organizaciones realizarán evaluaciones o auditorías periódicas, convenientemente documentadas, que garanticen la adecuación de la política de gestión documental y que los procesos de gestión de documentos electrónicos se realizan conforme a lo establecido en la política.

X.3 Los resultados de dichas evaluaciones serán considerados para la actualización de la política, programa de tratamiento y procesos de gestión de documentos electrónicos.

*XI. Actualización*

La política de gestión de documentos electrónicos, el programa de tratamiento y los procesos de gestión documental serán convenientemente actualizados con el fin de garantizar su adecuación permanente a las necesidades reales de gestión de documentos electrónicos y normativa aplicable.

# § 21

## Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas

Ministerio de Política Territorial y Administración Pública
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13173

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas se desarrolla bajo lo establecido en el artículo 43 de la Ley 11/2007, de 22 de junio, y artículo 13 del Real Decreto 4/2010, de 8 de enero, para posibilitar la interconexión de las redes de las Administraciones públicas y permitir el intercambio de información entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros.

La Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas establece las condiciones en las que cualquier órgano de una Administración, o Entidad de Derecho Público vinculada o dependiente de aquélla, accederá a la Red SARA, y describe los roles y responsabilidades de los agentes que se conectan a la Red SARA así como los requisitos para la conexión, acceso y uso de los servicios que se prestan a través de aquélla.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas, cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

## NORMA TÉCNICA DE INTEROPERABILIDAD DE REQUISITOS DE CONEXIÓN A LA RED DE COMUNICACIONES DE LAS ADMINISTRACIONES PÚBLICAS ESPAÑOLAS

### *I. Consideraciones generales*

I.1 *Objeto*.–La Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas tiene por objeto establecer las condiciones en las que cualquier órgano de una Administración, o Entidad de Derecho Público vinculada o dependiente de aquélla (en adelante, organización), accederá a la Red SARA.

I.2 *Ámbito de aplicación*.–El contenido de esta norma será de aplicación en la conexión a la Red SARA en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

### *II. Agentes y conexión a la Red SARA*

II.1 *Conexión a la Red SARA.*

1. El acceso a la Red SARA se realizará a través de lo que se denomina Punto de Presencia (PdP) entendido como cualquier sede en la que existe una conexión directa a la Red SARA, sin presencia de ninguna organización intermedia.

2. Entre los PdPs de la Red SARA podrán distinguirse los siguientes tipos:

a) Proveedores de Acceso a la Red SARA (PAS).

b) Centros de Proceso de Datos (CPD) de SARA.

c) Red sTESTA (secure Trans-European Services for Telematics between Administrations).

d) Centros externos de monitorización.

e) Prestadores de servicios de certificación.

f) Otros: como son las Ventanillas Únicas Empresariales.

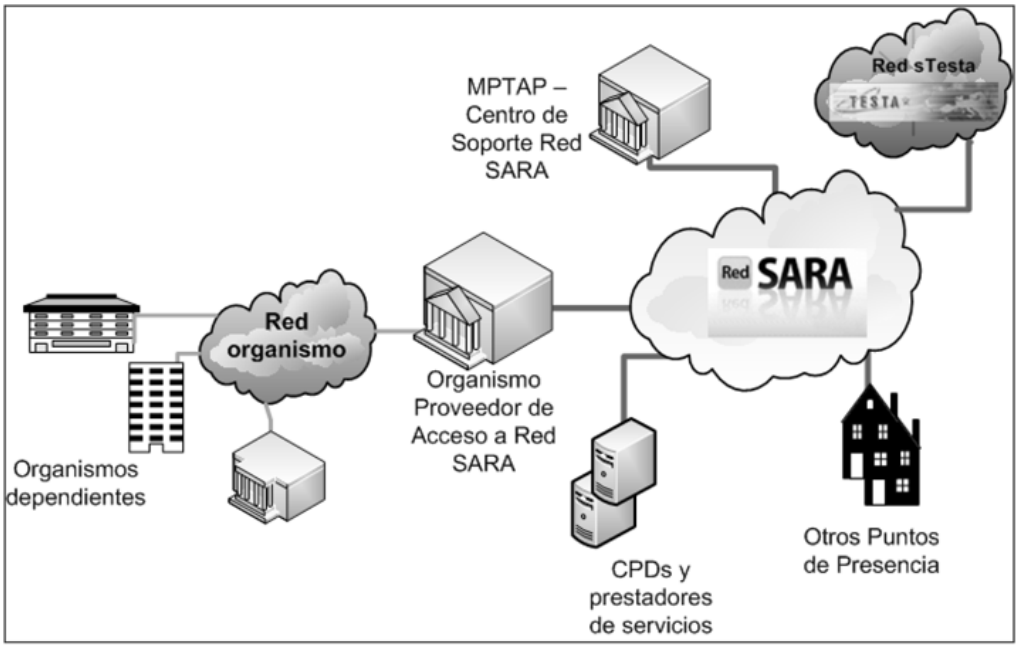



Figura 1. Puntos de Presencia y esquema de conexión a Red SARA

3. Con independencia de casos especiales de PdPs, en la conexión de cualquier organización a la Red SARA será necesaria la intervención del Ministerio de Política Territorial y Administración Pública (en adelante, MPTAP), un proveedor de acceso y la propia organización que desea conectarse, que actuará como usuario final.

II.2 *MPTAP-Centro de Soporte de la Red SARA.*–Las funcionalidades prestadas por el Centro de Soporte de la Red SARA del MPTAP se podrán consultar en el portal web www.redsara.es, accesible desde la Red SARA.

II.3 *Proveedores de Acceso a la Red SARA (PAS).*

1. La conexión directa a la Red SARA se proporcionará a través de un Área de Conexión (AC) que se ubicará en las dependencias de la Administración pública correspondiente convirtiéndose ésta en Proveedor de Acceso a la Red SARA (PAS) para sus Unidades, Organismos y Entidades de Derecho Público dependientes y, en el caso de las Comunidades Autónomas, también para las Administraciones Locales de su ámbito territorial.

2. Las organizaciones que no están adscritas a ningún organismo superior: Ministerios, Comunidades y ciudades con Estatuto de Autonomía y Órganos constitucionales, funcionarán como PAS a excepción de las Administraciones Locales que quedarán asignadas al PAS de la Comunidad Autónoma correspondiente.

3. Otros organismos públicos podrán asumir las funciones de PAS siempre que el MPTAP así lo establezca atendiendo a la singularidad del organismo o a la prestación, por parte de aquél, de servicios considerados singulares.

4. El establecimiento de un nuevo PAS, a solicitud del interesado, corresponderá al MPTAP a través del Centro de Soporte de la Red SARA.

II.4 *Órganos usuarios finales.*

1. Todo órgano usuario final de la Red SARA accederá a ésta a través de una organización que ejercerá las funciones de PAS.

2. Las características y dispositivos de la conexión de los órganos finales con el PAS correspondiente dependerán de las condiciones y mecanismos que disponga el propio PAS.

3. La solicitud de conexión de los órganos finales se dirigirá directamente al PAS del que dependen y será comunicada al Centro de Soporte de la Red SARA.

4. El listado completo de PAS estará disponible en el portal web www.redsara.es, accesible desde la Red SARA.

***III. Requisitos técnicos para la conexión del PAS***

III.1 *Esquema del Área de Conexión (AC).*

1. El AC de un PAS funcionará como punto único de conexión entre la red de la Administración pública correspondiente y sus organizaciones dependientes o asignadas al PAS, a las redes de otras administraciones y Entidades públicas conectadas a la Red SARA, así como a la Red sTESTA de la Comisión Europea.

2. La estructura del AC responderá al esquema de una zona desmilitarizada (DMZ) delimitada por un subsistema de seguridad externo, que conectará con el resto de la Red SARA, y un subsistema de seguridad interno hacia el interior de la organización.

3. Los elementos del AC, además de proporcionar seguridad perimetral, albergarán los servicios telemáticos básicos prestados por la Red SARA: DNS, SMTP, NTP, Proxy y Proxy inverso.

4. El subsistema de seguridad externo será el encargado de establecer una red privada virtual (VPN) hacia el resto de sedes de la Red SARA, con lo que todas las comunicaciones, a través del operador de servicios de telecomunicaciones, estarán cifradas mediante túneles.

5. En la zona intermedia, DMZ, será posible conectar cualquier equipo que la organización considere conveniente utilizar para la comunicación con el resto de organizaciones que componen la Red. Para no vulnerar la seguridad global de la Red, el Centro de Soporte de la Red SARA del MPTAP determinará las condiciones en que dichos elementos adicionales deberán integrarse en el AC.

6. Un esquema muy simplificado de un AC es el siguiente:

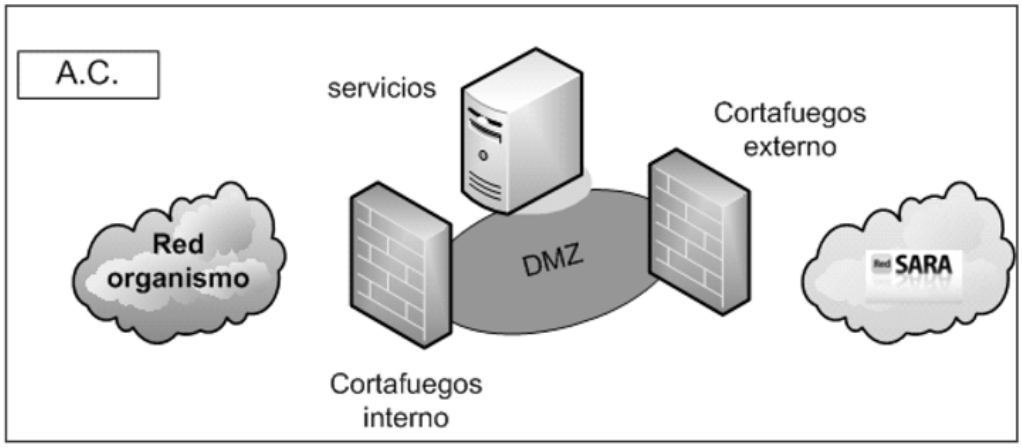



Figura 2. Esquema lógico de un Área de Conexión (AC)

III.2 *Administración de la conexión.*–El MPTAP administrará la conexión a la Red SARA y aplicará las políticas necesarias para el aseguramiento de la interoperabilidad y el nivel de seguridad correspondiente.

III.3 *Plan de direccionamiento.*

1. Las organizaciones que se conecten a la Red SARA aplicarán el Plan de direccionamiento e Interconexión de Redes en la Administración establecido por la Dirección General para el Impulso de la Administración Electrónica (DGIAE) disponible en http://administracionelectronica.gob.es/ según lo dispuesto en artículo 14 del Real Decreto 4/2010, de 8 de enero.

2. Todas las partes pondrán todos los medios a su alcance para adaptarse a los correspondientes planes de direccionamiento, de tal manera que un determinado rango o espacio de direcciones IP será reservado para preservar la compatibilidad e interoperabilidad.

III.4 *Dotación de elementos de conectividad.*–El MPTAP adquirirá, instalará, administrará, configurará y mantendrá los elementos de conectividad de cada PAS.

III.5 *Garantías de acondicionamiento físico.*–El acondicionamiento físico de las instalaciones del PAS cumplirá lo establecido a tal efecto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica de manera que se asegure la continuidad del servicio.

III.6 *Servicios de soporte y gestión de incidentes.*

1. El soporte y la gestión de incidentes de la Red SARA se prestarán de manera conjunta entre el MPTAP y los PAS, a través de sus correspondientes equipos dedicados a estos servicios.

2. Para facilitar la actuación conjunta entre el MPTAP y los PAS, cada organización proporcionará los siguientes datos de sus servicios de soporte y de gestión de incidentes:

a) Identificación.
b) Responsable de la unidad.
c) Responsable técnico.
d) Horario de servicio.
e) Localización.
f) Horario y datos de contacto para incidentes.
g) Observaciones.

3. Los datos identificativos y de contacto de los servicios de soporte y de gestión de incidentes de cada organización serán convenientemente actualizados y distribuidos entre todos los agentes de manera que se asegure la disponibilidad de la información de contacto para actuar ante cualquier incidente. Su consulta estará disponible a través del portal web www.redsara.es, accesible desde la Red SARA.

### *IV. Acceso y utilización de servicios*

IV.1 *Acceso a los servicios.*

1. Cualquier organización con conexión a la Red SARA, podrá solicitar la utilización de cualquiera de los servicios que se presten a través de ésta.

2. El catálogo de servicios disponibles en la Red SARA estará disponible en el portal web www.redsara.es, accesible desde la Red SARA.

IV.2 *Mantenimiento del catálogo de servicios.*

1. El catálogo de servicios será mantenido y actualizado por el MPTAP y el PAS a través del cual se presta cada servicio.

2. Todos los servicios que se publiquen en la Red SARA, a través de un PAS, serán comunicados al Centro de Soporte de la Red SARA con el fin de mantener el catálogo de servicios correctamente actualizado.

3. El catálogo de servicios facilitará la elaboración de estadísticas y cuadros de mando que el MPTAP podrá publicar en el portal web www.redsara.es y poner a disposición de todos los implicados.

IV.3 *Condiciones de utilización de los servicios.*

1. Para los servicios verticales o de negocio, así como para los servicios comunes de administración electrónica, con independencia de condiciones particulares que pudiese establecer el prestador del servicio, las condiciones de utilización serán

a) Acuerdo previo entre la Administración pública que presta el servicio y la beneficiaria.
b) Comunicación al Centro de Soporte de la Red SARA del MPTAP.
c) Si procede, condiciones de la plataforma de intermediación de datos que intervenga en el servicio. En caso de uso de la Plataforma de intermediación del MPTAP, se atenderá a lo establecido en la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos.

2. La solicitud de alta de un nuevo servicio y las comunicaciones al Centro de Soporte de la Red SARA se realizarán a través de los medios dispuestos para tal fin en el portal web www.redsara.es, donde figurarán, al menos, los siguientes datos:

a) Datos del solicitante.
b) Datos generales del servicio.

i. Nombre del servicio o aplicación.
ii. Nivel de criticidad.
iii. Horario de disponibilidad.
iv. Destinatarios del servicio.

c) Datos del soporte técnico para el contacto con dicho servicio.
d) Datos técnicos de acceso y uso del servicio.

***V. Agentes y roles***

V.1 *Ministerio de Política Territorial y Administración Pública.*–El MPTAP:

a) Instalará, administrará y mantendrá una conexión de capacidad suficiente y alta disponibilidad ubicada en las dependencias que la Administración pública determine y que mejor permita la conexión con su correspondiente red para constituirse como PAS.

b) Proporcionará a los responsables del PAS la documentación técnica correspondiente a la arquitectura y configuración de los sistemas que componen el AC.

c) Mantendrá un servicio de soporte 24x7 para garantizar la continuidad del servicio en el AC y la red troncal que sirva para realizar la gestión de incidentes y problemas, cuando le corresponda, así como la gestión de la resolución cuando intervengan agentes externos (fabricantes, operadores u otros organismos con acceso al sistema), consultas técnicas relacionadas con el servicio o peticiones de nuevos accesos.

d) Gestionará el portal web www.redsara.es, como espacio para facilitar información general sobre la Red SARA así como información específica para los responsables técnicos del PAS respecto del servicio proporcionado, notificación de incidencias, paradas programadas, publicación de nuevos servicios y otras informaciones de interés.

e) Adoptará las medidas de seguridad necesarias para proteger debidamente la información transmitida, mediante el cifrado de las comunicaciones y la detección temprana de incidentes en colaboración con el CCN-CERT.

V.2 *Proveedores de acceso a la Red SARA.*–Cualquier Administración pública que funcione como PAS:

a) Realizará las labores de conectividad y despliegue pertinentes para poder acceder desde sus propias dependencias o instalaciones a la Red SARA a través del AC.

b) Gestionará y mantendrá los elementos activos que conectan su red corporativa a la Red SARA.

c) Garantizará condiciones adecuadas en la ubicación del AC (condiciones medioambientales, suministro eléctrico, cableado, etc.) con el fin de asegurar la continuidad del servicio.

d) Mantendrá un servicio de soporte, a ser posible 24x7, para garantizar la continuidad del servicio en su función como PAS. Para ello se facilitarán al MPTAP los contactos, tanto de los responsables del PAS como los del Centro de Soporte, Centro de Atención al Usuario o equivalente.

e) Colaborará con el MPTAP en la gestión de incidentes y problemas, incluso si ello lleva consigo pequeñas comprobaciones o actuaciones en el AC, dirigidas desde el Centro de Soporte de la Red SARA, con el fin de reducir los tiempos de resolución de las incidencias que pudieran ocurrir.

f) Facilitará, promoverá y sostendrá el acceso a la Red SARA a sus Organismos y Entidades de Derecho Público dependientes y adicionalmente, en el caso de Comunidades Autónomas, a las Administraciones Locales de su ámbito territorial, con la tecnología, mecanismos y procedimientos que éstos acuerden, garantizando la continuidad del servicio y las condiciones adecuadas de seguridad en la parte que le corresponde.

g) Colaborará con el MPTAP en el mantenimiento del catálogo de servicios y conexiones.

V.3 *Órganos usuarios finales.*–Los Organismos y Entidades de Derecho Público dependientes y adicionalmente, en el caso de Comunidades Autónomas, las Administraciones Locales de su ámbito territorial, que disfruten del acceso a la Red SARA a través del PAS correspondiente, aplicarán:

a) Condiciones particulares del PAS del que dependen.
b) Condiciones particulares de servicios horizontales y verticales que utilizan a través de la Red SARA.

V.4 *Publicidad de referencias.*

1. El MPTAP podrá hacer pública, en cualquier lista de referencia o en cualquier boletín de prensa publicado y sin autorización previa, la relación de organismos usuarios de la Red SARA.
2. Las Administraciones públicas podrán referenciar la utilización de la Red SARA sin autorización previa por parte del MPTAP.

# § 22

## Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos

Ministerio de Política Territorial y Administración Pública
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13172

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

En particular, la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos establece las reglas para la generación y expedición de copias electrónicas auténticas, copias papel auténticas de documentos públicos administrativos electrónicos y para la conversión de formato de documentos electrónicos por parte de las Administraciones públicas; para los aspectos relativos a la gestión de los documentos resultantes del proceso de copiado auténtico o conversión, se remite a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

## NORMA TÉCNICA DE INTEROPERABILIDAD DE PROCEDIMIENTOS DE COPIADO AUTÉNTICO Y CONVERSIÓN ENTRE DOCUMENTOS ELECTRÓNICOS

### *I. Objeto*

La Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos tiene por objeto establecer las reglas para la generación de copias electrónicas auténticas, copias papel auténticas de documentos públicos administrativos electrónicos y para la conversión de formato de documentos electrónicos.

### *II. Ámbito de aplicación*

Esta norma será de aplicación en los procedimientos de copiado auténtico y conversión entre documentos electrónicos en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

### *III. Características generales de las copias electrónicas auténticas*

III.1 Las copias electrónicas generadas que, por ser idénticas al documento electrónico original no comportan cambio de formato ni de contenido, tendrán la eficacia jurídica de documento electrónico original.

III.2 Las copias auténticas se expedirán a partir de documentos con calidad de original o copia auténtica.

III.3 Las copias electrónicas auténticas serán nuevos documentos electrónicos que incluirán total o parcialmente el contenido del documento sobre el que se expiden y que

cumplirán con lo establecido en la Norma Técnica de Interoperabilidad de Documento electrónico.

III.4 El valor de cada uno de los metadatos mínimos obligatorios del documento electrónico copia será asignado en función de las características propias de cada metadato y de las propiedades específicas del documento bajo la responsabilidad del órgano u Organismo que lo expide.

III.5 La relación entre la copia electrónica auténtica y el documento origen se reflejará en los metadatos del documento electrónico copia a través del metadato «Identificador del documento origen» que tomará el valor del identificador de aquél.

III.6 Las copias electrónicas auténticas serán firmadas mediante alguno de los sistemas de firma previstos en los artículos 18 ó 19 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

*IV. Copia electrónica auténtica con cambio de formato*

Las copias electrónicas auténticas con cambio de formato:

1. Se obtendrán de la aplicación de una conversión entre documentos electrónicos que se realizará según lo establecido en el apartado VIII de esta norma.

2. Tendrán asignado el valor «Copia electrónica auténtica con cambio de formato» en el metadato mínimo obligatorio «Estado de elaboración».

*V. Copia electrónica auténtica de documentos papel*

Las copias electrónicas auténticas de documentos en soporte papel o en otro soporte no electrónico susceptible de digitalización a través de medios fotoeléctricos:

1. Se obtendrán de la digitalización del documento origen según lo establecido en la Norma Técnica de Interoperabilidad de Digitalización de documentos.

2. Tendrán asignado el valor «Copia electrónica auténtica de documento papel» al metadato mínimo obligatorio «Estado de elaboración».

*VI. Copia electrónica parcial auténtica*

Las copias electrónicas parciales auténticas:

1. Se obtendrán mediante extractos del contenido del documento origen que corresponda o a través de la utilización de otros métodos electrónicos que permitan mantener la confidencialidad de aquellos datos que no afecten al interesado.

2. Tendrán asignado el valor «Copia electrónica parcial auténtica» en el metadato mínimo obligatorio «Estado de elaboración».

*VII. Copia papel auténtica de documentos públicos administrativos electrónicos*

Para la obtención de copias auténticas en soporte papel de documentos públicos administrativos electrónicos se atenderá a lo previsto en la normativa aplicable y a lo establecido sobre el acceso a documentos electrónicos en la Norma Técnica de Interoperabilidad de Documento electrónico para la verificación de su autenticidad.

*VIII. Conversión entre documentos electrónicos*

VIII.1 La conversión entre documentos electrónicos supondrá la generación de un nuevo documento electrónico con diferente formato o versión a la del documento origen que cumplirá con lo establecido en la Norma Técnica de Interoperabilidad de Documento electrónico.

VIII.2 La conversión entre documentos electrónicos se realizará atendiendo a:

a) La aplicación de procedimientos de conversión establecidos en un marco de gestión documental definido según la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

b) La conservación del contenido, contexto y estructura del documento origen e identificación de componentes que requieran, dada su naturaleza, un tratamiento específico en la conversión.

c) El formato del nuevo documento convertido será seleccionado de entre los establecidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares y permitirá la reproducción de la información contenida en el documento original minimizando el riesgo de pérdida de información.

VIII.3 En el caso de que el documento resultado de la conversión deba ser conformado como copia auténtica, se contemplarán, adicionalmente, los requisitos establecidos en los apartados III y IV de esta norma.

# § 23

## Resolución de 22 de julio de 2021, de la Secretaría de Estado de Digitalización e Inteligencia Artificial, por la que se aprueba la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las entidades registrales

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 190, de 10 de agosto de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-13749

El Esquema Nacional de Interoperabilidad (ENI) se establece en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que sustituye al apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia, en el marco, entre otras normas, de la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas.

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano.

En particular, la Norma Técnica de Interoperabilidad de Modelo de Datos para el Intercambio de asientos entre las entidades registrales se aprobó mediante Resolución de 19

de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, para responder a lo recogido en el artículo 24.4 de la Ley 11/2007, de 22 de junio, sobre garantía de interconexión de todas oficinas de registro y posibilitar el acceso por medios electrónicos a los asientos registrales y a las copias electrónicas de los documentos presentados.

Posteriormente, la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y las previsiones recogidas en su artículo 16.4, que establece que los registros electrónicos de todas y cada una de las Administraciones, deberán ser plenamente interoperables, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de los asientos registrales y de los documentos que se presenten en cualquiera de los registros, hacen necesario la actualización de esta Norma Técnica de Interoperabilidad.

Así, la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales, que sustituye a la anterior, normaliza los intercambios registrales entre las oficinas de registro para garantizar su interoperabilidad y, como novedad, permite la adecuación de los intercambios a las nuevas necesidades de las oficinas de registro y favorece el avance hacia una tramitación automatizada de la documentación intercambiada.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por el Comité de Dirección de Tecnologías de la Información y Comunicaciones y por la Comisión Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales (SICRES4), que sustituye a la anterior Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales (SICRES3) de 2011, y cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales (SICRES4) que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Desde su publicación en el «Boletín Oficial del Estado» se dispondrá de un año para la adaptación de la anterior Norma Técnica de Interoperabilidad. Durante ese período, ambas versiones estarán vigentes.

## NORMA TÉCNICA DE INTEROPERABILIDAD DE MODELO DE DATOS PARA EL INTERCAMBIO DE ASIENTOS ENTRE LAS ENTIDADES REGISTRALES

### *I. SICRES: Sistema de Información Común de Registros de Entrada y Salida*

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante, Ley 30/1992), estableció por primera vez la posibilidad de que las Administraciones públicas utilizaran medios electrónicos y telemáticos en su relación con el ciudadano. Dentro de este ámbito se incluía inicialmente la integración informática de los registros generales con los restantes registros administrativos (artículo 38.3 de la Ley 30/1992, de 26 de noviembre).

Posteriormente, el legislador amplió las potestades de las Administraciones en este ámbito a través de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, que venía a añadir un nuevo apartado al ante dicho artículo 38 por el que

se reconocía «la posibilidad de crear registros telemáticos para la recepción o salida de solicitudes, escritos y comunicaciones que se transmitan por medios telemáticos».

Siguiendo el espíritu de la Ley 30/1992, de 26 de noviembre, el Consejo Superior de Informática (en adelante, CSI), en aquel momento Consejo Superior de Administración Electrónica según el Real decreto 589/2005, (en adelante, CSAE), definió en 1995 por primera vez, el estándar SICRES versión 1.0 (Sistemas de Información Común de Registros de Entrada y Salida) por el que se fijaban los criterios que debían cumplir todos los sistemas de Registro que se implantaran en la Administración, versión que fue actualizada en 1999 por el CSI a través de la norma SICRES versión 2.0.

En definitiva, con la definición de SICRES se perseguía lograr una tramitación más eficaz de los expedientes a través de un Registro Central interconectado con las distintas oficinas registrales y garantizar los derechos que la citada Ley 30/1992 reconocía.

Posteriormente, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicio Públicos, volvió a ratificar la regulación de los registros electrónicos administrativos y la interconexión de estos. Así, el artículo 24 de esta ley, estableció que las Administraciones Públicas crearían registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.

En 2010, se aprobó el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, el cual es de aplicación a todas las Administraciones Públicas. En el artículo 25 de este Real Decreto, se establece que los registros electrónicos deben regirse por lo establecido en el Esquema Nacional de Interoperabilidad, y por tanto también por las Normas Técnicas de Interoperabilidad aprobadas a raíz de este.

Así, se aprobó en 2010, con aplicación a todas las Administraciones Públicas, la Norma Técnica de Interoperabilidad de Modelo de Datos para el Intercambio de asientos entre las Entidades Registrales, la cual aprobaba la versión 3 de la norma SICRES. Esta norma SICRES3.0 presentaba las principales diferencias con respecto a sus predecesoras:

i. Orientación a arquitectura de intermediación.
ii. Incorporación de ficheros adjuntos a los intercambios.
iii. Mejora en los mecanismos de control del intercambio.

### *II. Objetivo y alcance de esta Norma Técnica de Interoperabilidad*

El objetivo de la Norma Técnica de Interoperabilidad (en adelante, NTI) de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales es definir las condiciones y características para la interconexión de registros de las Administraciones públicas, y, por tanto, el intercambio de información entre estas.

Para ello, esta NTI contiene la especificación SICRES 4.0, evolución de su antecesora SICRES 3.0,

Su contenido abarca los siguientes puntos:

i. Definición y características principales de SICRES 4.0
ii. Esquema de datos y formatos para los ficheros intercambiados.
iii. Mecanismos de control y gestión de errores a aplicar en el proceso.
iv. Prestaciones de alto nivel a garantizar por el sistema de intercambio utilizado.

### *III. Ámbito de aplicación y destinatarios*

El contenido de esta NTI es de aplicación para todos los órganos de la Administración pública o Entidades de derecho Público vinculadas o dependientes de aquélla (en adelante, organizaciones) que participan en el intercambio de asientos registrales, ya sea para la prestación de servicios directos a los ciudadanos, como de cara al intercambio de información con otros órganos.

Dentro del ámbito de aplicación definido, los destinatarios del contenido de esta norma son los siguientes:

i. Responsables de sedes electrónicas y, por tanto, de garantizar los requisitos de interoperabilidad de las mismas y, concretamente, de sus registros electrónicos.

ii. Responsables y administradores de aplicaciones, redes y servicios corporativos de cualquier órgano.

***IV. Modelo de datos para el intercambio de asientos entre Entidades Registrales***

IV.1 Definición y características generales de SICRES 4.0.

SICRES 4.0 constituye el modelo de datos para el intercambio de asientos entre Entidades Registrales. Esta versión de SICRES, alineada con la filosofía de sus predecesoras, tiene como finalidad contribuir a garantizar la interconexión entre organizaciones, permitiendo así, un servicio de mayor calidad a los ciudadanos tal y como marca la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Las principales características de SICRES 4.0 que la diferencian de sus versiones anteriores son:

i. Reordenación, actualización e incorporación de campos. El modelo de intercambio SICRES 4.0 agrupa y reordena los campos de los distintos segmentos para dotarlos de mayor contenido semántico y facilitar su interpretación. Asimismo, se eliminan o actualizan campos obsoletos y se incorporan nuevos campos.

ii. Referenciación de documentos electrónicos. Se sustituye el intercambio de los ficheros de los documentos electrónicos objeto de registro e intercambio, por el intercambio de referencias a tales documentos electrónicos. De este modo, se optimiza el funcionamiento de la Plataforma de Intercambio y se superan limitaciones de la misma.

iii. Metadatado para automatización del tratamiento de los asientos registrales y sus documentos anexos. Se incorporan en el intercambio registral nuevos metadatos destinados a facilitar la automatización del tratamiento de los asientos y los documentos electrónicos. Asimismo, se incorpora la posibilidad de intercambiar otros metadatos no definidos a priori, bien sea para cubrir necesidades futuras, o bien sea para cubrir necesidades particulares de cada organismo.

Durante el período de transición de las aplicaciones de registro de SICRES 3.0 a SICRES 4.0 se garantizará la interoperabilidad entre ambas normas. La plataforma de intercambio de asientos registrales SIR se encargará de garantizar la compatibilidad y la comunicación entre aplicaciones de registro que utilicen diferentes versiones de la norma.

El modelo conceptual de espacio de intercambio bajo SICRES 4.0 aparece en la siguiente figura:

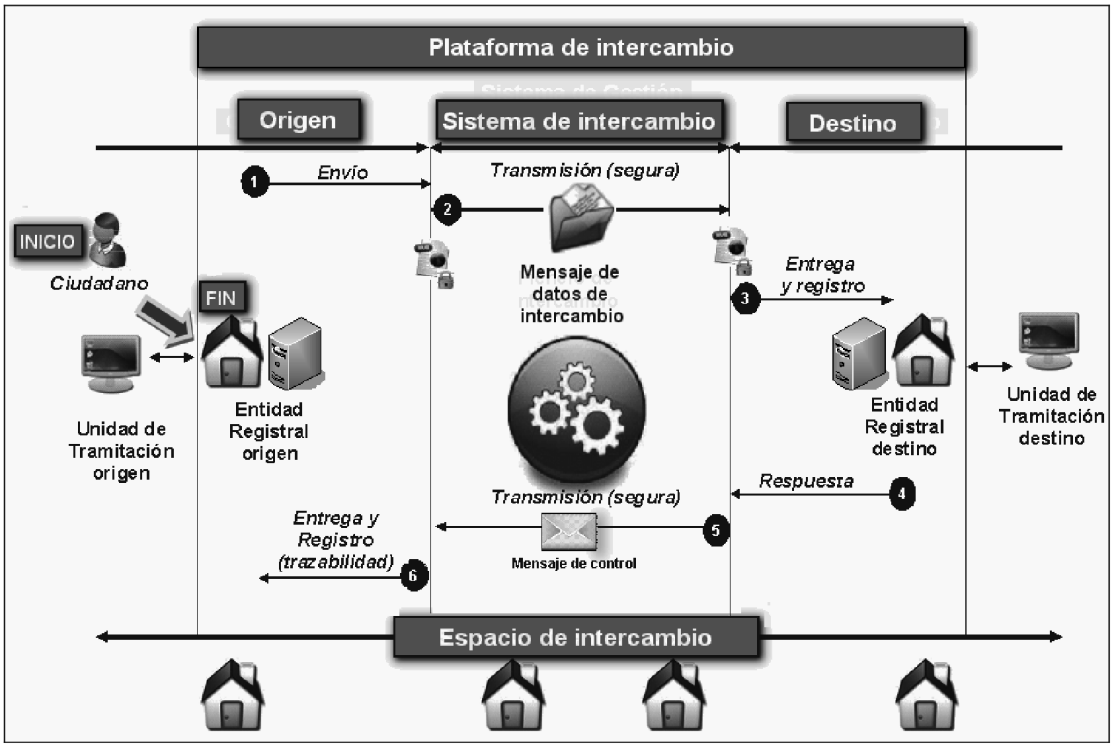



**Figura 1.** Esquema del modelo de intercambio de SICRES 4.0

Según este esquema, el espacio de intercambio engloba todo el proceso de intercambio desde la Unidad de Tramitación Origen hasta la Unidad Tramitación Destino proporcionando un contexto único a cada uno de los intercambios. Dentro de este espacio, destacan los siguientes elementos:

Unidades de Tramitación de Origen y Destino: Entidades, o unidades pertenecientes a dichas entidades, responsables de la tramitación de los documentos registrados. La identificación de ambas Unidades debe ser única a través de Directorios unificados, como se indica en el apartado VI.4 de esta norma.

Entidad Registral de Origen y Destino. Entidades, o unidades pertenecientes a dichas entidades, que, bien sea por medio del personal al servicio del mismo, o bien sea por medio de actuación automatizada, se encarga tanto de inscribir los asientos de entrada y salida en el Registro Electrónico de la Administración u Organismo, como de llevar a cabo el proceso de intercambio registral, responsabilizándose del envío y recepción de Mensajes de Datos de Intercambio y Mensajes de Control, desde el punto de vista técnico y de comunicación, pero sin implicación en la tramitación de los documentos. La identificación de ambas Entidades Registrales debe ser única a través de Directorios unificados, como se indica en el apartado VI.4 de esta norma.

Mensaje de datos de intercambio. Es creado y emitido por la Entidad Registral de Origen y alberga, además de campos para el control e identificación, la información del asiento registral y los documentos correspondientes adjuntos. Su estructura y formato se definen en el apartado IV.2 de esta norma.

Mensajes de control. Son emitidos por la Entidad Registral destino o por el propio sistema de intercambio y proporcionan información de estado para la gestión de la operación de intercambio. Su estructura y formato se definen en el apartado IV.3 de esta norma.

Sistema de intercambio. Proporciona la gestión del intercambio y la comunicación directa con las Entidades Registrales Origen y Destino. Sus funciones y requisitos técnicos deben cumplir lo establecido en el apartado VI de esta norma.

Plataforma de intercambio. Comprende el Sistema de intercambio y las Entidades Registrales de Origen y de Destino.

El proceso de intercambio inicia y finaliza en la Entidad Registral de Origen, punto de contacto con el ciudadano o Unidad de Tramitación que origina la creación del asiento registral.

El inicio viene marcado por la generación del mensaje de datos de intercambio en la Entidad Registral Origen conteniendo la información del asiento. A través del sistema de intercambio, este mensaje es recibido en la Entidad Registral destino, que, si procede, confirma la recepción correcta al Origen a través del mensaje de control correspondiente.

Los intercambios disfrutan de un contexto único dentro del espacio SICRES mediante la asignación de un identificador del intercambio único a cada proceso de transacción que es generado por la aplicación de registro de la Entidad Registral de Origen y acompaña tanto al mensaje de datos de intercambio como a los mensajes de control relacionados. La generación del identificador del intercambio se detalla en el apartado V.1 de esta NTI.

IV.2 Estructura y contenido del mensaje de datos de intercambio.

El mensaje de datos de intercambio de SICRES4.0 es el mensaje que alberga la información objeto del intercambio. Su codificación se especifica con un ejemplo de implementación del modelo en XML en el Anexo 2 de esta norma.

Este mensaje está compuesto por los 7 segmentos que aparecen en la figura y cuya descripción funcional se desarrolla a continuación.

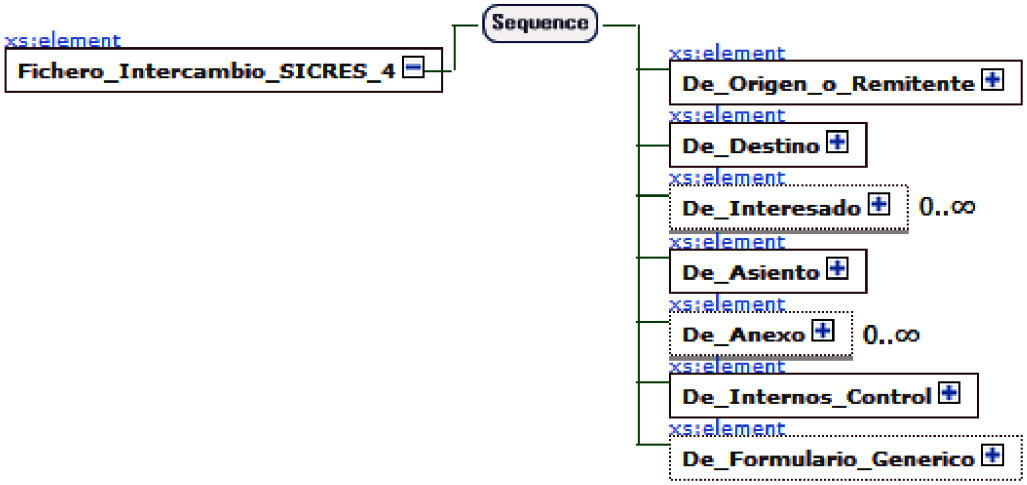



**Figura 2.** Estructura del fichero de intercambio de SICRES 4.0

Segmento de Origen (o Remitente).

| Segmento de Origen (o Remitente) | | | | ☑ Obligatorio ☑ Único |
|---|---|---|---|---|
| SICRES 4.0 | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Código Entidad Registral de Origen. | Alfanumérico. | 21 | Obligatorio. | Código único obtenido de Directorios Unificados indicados en el apartado VI.4. |
| Decodificación de Entidad Registral de Origen. | Alfanumérico. | 120 | Opcional. | Descripción de la Entidad Registral de Origen. |
| Código de la Unidad de Tramitación de Origen. | Alfanumérico. | 21 | Condicional. | Código único obtenido de Directorios Unificados indicados en el apartado VI.4. La cumplimentación de este campo es obligatoria cuando el emisor del registro es un órgano u organismo perteneciente o dependiente de una Administración Pública. |
| Decodificación de la Unidad de Tramitación de Origen. | Alfanumérico. | 120 | Opcional. | Descripción de la Unidad de Tramitación Origen. |

Tabla 1. Datos de Origen (o Remitente)

La cumplimentación de la Unidad de Tramitación de Origen será obligatoria cuando el emisor del registro sea un órgano u organismo perteneciente o dependiente de una Administración Pública, como se indica en el comentario del campo.

Sin embargo, no será obligatoria la cumplimentación de este campo en los reenvíos o rechazos que se realicen de registros emitidos por Administraciones Públicas. Asimismo, tampoco será obligatoria la cumplimentación, en envíos registrales que se traten de rectificaciones de intercambios previos. Es decir, en envíos registrales que realicen órganos y organismos de las Administraciones Públicas como consecuencia de haber confirmado por error un registro que habían recibido.

B) Segmento de destino.

| **Segmento de destino (o destinatario)** | | | | **☑ Obligatorio<br>☑ Único** |
|---|---|---|---|---|
| **SICRES 4.0** | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Código Entidad Registral de Destino. | Alfanumérico. | 21 | Obligatorio. | Código único obtenido de Directorios Unificados indicados en el apartado VI.4. |
| Decodificación Entidad Registral de Destino. | Alfanumérico. | 120 | Opcional. | Descripción de Entidad Registral de destino. |
| Código de la Unidad de Tramitación de Destino. | Alfanumérico. | 21 | Condicional. | Código único obtenido de Directorios Unificados indicados en el apartado VI.4. La cumplimentación de este campo es obligatoria cuando el destinatario del registro es un órgano u organismo perteneciente o dependiente de una Administración Pública. |
| Decodificación de la Unidad de Tramitación de Destino. | Alfanumérico. | 120 | Opcional. | Descripción de la Unidad de Tramitación de destino. |

Tabla 2. Datos de destino

C) Segmento de Interesado.

Este segmento comprende los datos que identifican al Interesado y su Representante en la entidad mensaje de datos de intercambio. Este segmento se puede declarar de forma múltiple. Su condicionalidad se define en los comentarios de los campos «Datos del Interesado» y «Datos del Representante».

| **Segmento de Interesado** | | | | **☑ Condicional<br>☑ Múltiple** |
|---|---|---|---|---|
| **SICRES 4.0** | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Datos del Interesado. | Tipo complejo. (Datos Persona). | | Condicional. | Este campo comprende todos los datos personales del interesado; tanto datos de identidad, como datos de contacto e información relativa a los canales de notificaciones.<br>Este campo deberá cumplimentarse siempre que el intercambio se realice en el marco de un procedimiento administrativo en el cual existe y se conoce el interesado.<br>En cualquier caso, será obligatorio siempre que se trate de un registro de entrada.<br>También deberá tenerse en cuenta que será obligatorio siempre que se indique Representante.<br>Estos campos deberán cumplimentarse con independencia de que la información sea redundante con la ya indicada en los Segmentos de Origen o Destino.<br>Se compone de los siguientes campos: *Datos de identificación*, *Datos de contacto*, *Receptor notificaciones* y *Canales de notificación.* |
| Datos del Representante. | Tipo complejo. (Datos Persona). | | Condicional. | Este campo comprende todos los datos personales del representante; tanto datos de identidad, como datos de contacto e información relativa a los canales de notificación.<br>Este campo no podrá cumplimentarse si no se ha cumplimentado el campo «Datos del Interesado».<br>Se compone de los siguientes campos: *Datos de identificación*, *Datos de contacto*, *Receptor notificaciones* y *Canales de notificación.* |
| Observaciones. | Alfanumérico. | 160 | Opcional. | Observaciones del Interesado y/o del Representante. |
| Tipo complejo: Datos Persona. | | | | |
| Datos de identificación. | Tipo complejo. (Datos Identificación). | | Obligatorio. | Se compone de los siguientes campos: «*Tipo de persona*», «*Tipo de Documento de Identificación*», «*Documento de Identificación*», «*Razón social*», «*Código de Directorios Unificado*», «*Nombre*», «*Primer apellido*» y «*Segundo apellido*». |
| Datos de contacto. | Tipo complejo (Datos Contacto). | | Opcional. | Se compone de los siguientes campos: «*Dirección postal*», «*Dirección Electrónica Habilitada*», «*Correo electrónico*», «*Teléfono*» y «*Teléfono móvil*». |
| Receptor de notificaciones. | Booleano. | | Opcional. | En escenarios con múltiples interesados y/o representantes, por medio de los valores booleanos «true» o «false», permite seleccionar expresamente cuál de los interesados o representantes será el que reciba las notificaciones. Tal y como el artículo 7 de la Ley 39/2015, por defecto, las notificaciones se remitirán al primer interesado que se consigne. |
| Canales de notificación y aviso. | Tipo complejo. (Canales Notificación). | | Opcional. | De acuerdo con la Ley 39/2015, permite indicar preferencias en cuanto a los canales de recepción de notificaciones y avisos de notificaciones. |
| Tipo complejo: Datos Identificación. | | | | |
| Tipo de persona. | Alfanumérico. | 1 | Obligatorio. | «1» = Persona física.<br>«2» = Persona jurídica. |

| Segmento de Interesado | | | | ☑ Condicional<br>☑ Múltiple |
|---|---|---|---|---|
| SICRES 4.0 | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Tipo de Documento de Identificación. | Alfanumérico. | 1 | Obligatorio. | Identificación del interesado o representante:<br>'N' = NIF.<br>'C' = CIF.<br>'P' = Pasaporte.<br>'E' = Documento de identificación de extranjeros.<br>'X' = Otros de persona física.<br>'O' = Código de Origen. |
| Documento de Identificación. | Alfanumérico. | 256 | Obligatorio. | Alfanumérico con la sintaxis adecuada en función del campo «Tipo de Documento de Identidad». |
| Razón Social. | Alfanumérico. | 80 | Condicional. | Obligatorio si es persona jurídica. |
| Código de Directorios Unificados. | Alfanumérico. | 21 | Opcional. | Código del Interesado dentro de alguno de los Directorios Unificados contemplados en el Apartado VI.4 de esta norma. Dependiendo del directorio empleado, permitirá, entre otros, obtener información complementaria del interesado o identificar unidades dentro de la estructura jerárquica en la que se pueda descomponer el interesado. |
| Nombre. | Alfanumérico. | 30 | Condicional. | Obligatorio si es persona física. |
| Primer apellido. | Alfanumérico. | 30 | Condicional. | Obligatorio si es persona física. |
| Segundo apellido. | Alfanumérico. | 30 | Opcional. | |
| Tipo complejo: Datos Contacto. | | | | |
| Dirección postal. | Tipo complejo. (Dirección Postal). | | Condicional. | Se compone de los siguientes campos: «País», «Provincia», «Municipio», «Dirección» y «Código Postal».<br>Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación. |
| Correo electrónico. | Alfanumérico. | 160 | Condicional. | Dirección de correo electrónico.<br>Obligatorio cumplimentarlo si se solicita aviso de puesta a disposición de la notificación por correo electrónico. |
| Teléfono móvil. | Alfanumérico. | 20 | Condicional. | Obligatorio cumplimentarlo si se solicita aviso de puesta a disposición de la notificación por SMS. |
| Teléfono fijo. | Alfanumérico. | 20 | Opcional. | |
| Tipo complejo: Dirección Postal. | | | | |
| País. | Alfanumérico. | 4 | Condicional. | Atributo según catálogo del INE.<br>Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación. |
| Provincia. | Alfanumérico. | 2 | Condicional. | Atributo según catálogo del anexo de la OM del Padrón (11/7/1997).<br>Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación y el país es España. |
| Municipio. | Alfanumérico. | 5 | Condicional. | Atributo según catálogo del anexo de la OM del Padrón (11/7/1997).<br>Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación y el país es España. |
| Dirección. | Alfanumérico. | 160 | Condicional. | Dirección.<br>Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación. |
| Código postal. | Alfanumérico. | 5 | Condicional. | Atributo según catálogo del anexo de la OM del Padrón (11/7/1997).<br>Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación y el país es España. |
| Tipo complejo: Canales Notificación. | | | | |
| Canal preferente de notificación. | Alfanumérico. | 1 | Opcional. | Permite indicar, en el caso de personas físicas, el canal preferente para la recepción de las notificaciones, de acuerdo con la Ley 39/2015:<br>«1» = Notificación en papel.<br>«2» = Notificación por medios electrónicos (siendo la administración quién, para cada trámite, decidirá si se efectúa por comparecencia en sede electrónica o en DEHú,o en ambas, pero debiendo ser en todo caso accesible desde el Punto de Acceso General). |
| Solicita aviso de notificación por SMS. | Booleano. | | Opcional. | Permite al interesado indicar si desea recibir por este canal aviso de puesta a disposición de la notificación. |
| Solicita aviso de notificación por correo electrónico. | Booleano. | | Opcional. | Permite al interesado indicar si desea recibir por este canal aviso de puesta a disposición de la notificación. |

Tabla 3. Datos de Interesado

Los campos «Dirección postal», «Correo electrónico» o «Teléfono móvil» son condicionales de modo que, se pueden cumplimentar voluntariamente, en cualquier caso, pero deben cumplimentarse obligatoriamente si el canal de contacto en cuestión ha sido seleccionado expresamente en el campo «Canal preferente de notificaciones», en «Solicita aviso de puesta a disposición de la notificación por correo electrónico» o en «Solicita aviso de puesta a disposición de la notificación por SMS», respectivamente.

El campo «Canal preferente de notificaciones» no podrá tener el valor «1» para interesados obligados a relacionarse electrónicamente con las administraciones.

D) Segmento de Asiento.

| Segmento de Asiento | | | | ☑ Obligatorio<br>☑ Único |
|---|---|---|---|---|
| SICRES 4.0 | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Modo de registro. | Alfanumérico. | 2 | Obligatorio. | "01" = Registro presencial en Oficina de Asistencia en Materia de Registro.<br>"02" = Registro electrónico (desde sede electrónica, registros electrónicos generales o particulares u otros servicios electrónicos). |

| Segmento de Asiento | | | | ☑ Obligatorio<br>☑ Único |
|---|---|---|---|---|
| SICRES 4.0 | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Tipo del registro. | Alfanumérico. | 1 | Obligatorio. | "0" = Registro de entrada.<br>"1" = Registro de salida. |
| Número de registro en la Entidad Registral de Origen o Inicio. | Alfanumérico. | 20 | Obligatorio. | Número de registro en la Entidad Registral de Origen o Inicio. |
| Fecha y hora de registro en Origen o Inicio. | Alfanumérico. | 19 | Obligatorio. | Formato AAAAMMDDHHMMSSZ. |
| Timestamp de registro en Origen o Inicio. | Alfanumérico. | Variable | Opcional. | Sello de tiempo del registro en Origen o Inicio. |
| Fecha y hora de presentación por el interesado. | Alfanumérico. | 19 | Obligatorio. | Formato AAAAMMDDHHMMSSZ. Coincidirá con la de registro si se registra en el mismo momento en el que se presenta por el interesado. |
| Timestamp de presentación por el interesado. | Alfanumérico. | Variable | Opcional. | Sello de tiempo de la presentación por el interesado. |
| «Abstract» o Resumen. | Alfanumérico. | 240 | Obligatorio. | |
| Código SIA. | Alfanumérico. | | Opcional. | Código del procedimiento o servicio en el marco del cual se realiza la tramitación administrativa. Se obtendrá del Sistema de Información Administrativa. |
| Número de expediente. | Alfanumérico. | | Opcional. | Número del expediente objeto de la tramitación administrativa.<br>Deberá emplearse el formato normalizado de Identificador de expediente establecido en la NTI de Expediente Electrónico. |
| Código de asunto según destino. | Alfanumérico. | 16 | Opcional. | Codificación del asunto en destino, si la solicitud incluye ese dato. Se procurará definir solicitudes que incluyan el código para permitir el manejo automatizado del asiento en destino. |
| Referencia externa. | Alfanumérico. | 16 | Opcional. | Cualquier referencia que el destino precise conocer y sea conocida por el solicitante (matrícula de vehículo, número de recibo cuyo importe se reclama, etc.). |
| Otros metadatos generales. | Tipo complejo. (Metadatos). | | Condicional. | Secuencia de campos del tipo «Campo» y «Valor» empleados para transmitir atributos del asiento que atiendan a necesidades generales. |
| Otros metadatos particulares. | Tipo complejo. (Metadatos). | | Opcional. | Secuencia de campos del tipo «Campo» y «Valor» empleados para transmitir atributos del asiento que atiendan a necesidades particulares de la Unidad de Tramitación de Destino. |
| Tipo complejo: Metadatos. | | | | |
| Campo. | Alfanumérico. | 80 | Opcional. | Nombre del metadato (general o particular) que se intercambia. |
| Valor. | Alfanumérico. | Variable | Opcional. | Valor del metadato (general o particular) indicado en el campo «Campo» anterior. |

Tabla 4. Datos de Asunto

El formato de las fechas y horas de registro y presentación es yyyyMMddHHmmssZ, donde Z representa la variación en horas y minutos respecto a GMT (Ejemplo: 20200917124020+0200).

Los campos «Otros metadatos generales», «Otros metadatos particulares», «Campo» y «Valor» permiten intercambiar otros metadatos relativos al asiento adicionales a los ya transmitidos en campos nativos de la norma SICRES.

En el caso de «Otros metadatos generales», el listado de atributos a intercambiar (es decir, el listado de posibles contenidos del campo «Campo») será acordado y fijado por las Administraciones Públicas, con independencia de la aprobación de la NTI y pudiendo ser modificado a lo largo del tiempo. Los atributos de este listado podrán tener carácter opcional, condicional u obligatorio, por lo que deberán ser implementados por todas las Entidades Registrales.

En el caso de «Otros metadatos particulares», el listado de atributos a intercambiar (es decir, el listado de posibles contenidos del campo «Campo») será determinado por la Unidad de Tramitación de Destino que lo desee atendiendo a sus necesidades particulares, pudiendo establecerse un único listado a emplear por todos los orígenes, o listados particulares para determinados orígenes. Estos atributos serán siempre opcionales.

E) Segmento de Anexo.

Este segmento comprende datos e información relativa a los documentos electrónicos que son objeto de registro e intercambio. En el caso de justificantes de registro, su intercambio como documento anexo es opcional.

El segmento contiene la referencia única del documento electrónico a intercambiar. Esta referencia única consiste en un conjunto de campos con metadatos que permiten al destino la identificación unívoca del documento, la localización del repositorio en el que se encuentra almacenado y, en su caso, la acreditación de permisos para su acceso. Los campos y formatos de la referencia única del documento serán acordados y establecidos por las Administraciones Públicas al margen de esta NTI y pudiendo ser modificados a lo largo del tiempo. Esta información se recoge en la «Especificación del Sistema de referenciación de

documentos en las AAPP» del Foro por el Documento Electrónico – Documentación para la Tramitación Automatizada (https://administracionelectronica.gob.es/comunidades/verPestanaDocumentacion.htm?idComunidad=141).

Este segmento es opcional y puede declararse de forma múltiple.

| **Segmento de Anexo** | | | | **☑ Opcional ☑ Múltiple** |
|---|---|---|---|---|
| **SICRES 4.0** | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Nombre del fichero anexado. | Alfanumérico. | 80 | Obligatorio. | Nombre del fichero original, incluyendo la extensión del fichero. |
| Identificador de fichero. | Alfanumérico. | 50 | Obligatorio. | Se compondrá siguiendo la normalización definida en el Anexo 1B. |
| Tipo de anexo. | Alfanumérico. | 2 | Obligatorio. | Indica el tipo de documento:<br>– '01' = Justificante de registro.<br>– '02' = Documento adjunto.<br>– '03' = Otro. |
| Tipo MIME. | Alfanumérico. | 80 | Opcional. | Tipo del fichero Anexo. |
| Anexo. | Tipo complejo (Especificación del Sistema de referenciación de documentos en las AAPP). | | Opcional. | Metadatos y referencia al documento electrónico registrado e intercambiado. Su estructura cumplirá la Especificación del Sistema de referenciación de documentos en las AAPP. |
| Resumen. | Alfanumérico. | 160 | Opcional. | Texto con descripción breve del contenido y naturaleza del anexo. |
| Código del formulario. | Alfanumérico. | 80 | Opcional. | Código del formulario o documento normalizado anexado. |
| Otros metadatos generales. | Tipo complejo. (Metadato). | | Opcional. | Secuencia de campos del tipo «Campo» y «Valor» empleados para transmitir atributos del anexo que atiendan a necesidades generales. |
| Otros metadatos particulares. | Tipo complejo. (Metadato). | | Condicional. | Secuencia de campos del tipo «Campo» y «Valor» empleados para transmitir atributos del anexo que atiendan a necesidades particulares de la Unidad de Tramitación de Destino. |
| Observaciones. | Alfanumérico. | 160 | Opcional. | Observaciones del fichero adjunto. |
| Tipo complejo: Metadato. | | | | |
| Campo. | Alfanumérico. | 80 | Opcional. | Nombre del metadato (general o particular) que se intercambia. |
| Valor. | Alfanumérico. | Variable | Opcional. | Valor del metadato (general o particular) indicado en el campo «Campo» anterior. |

Tabla 5. Datos de Anexo

F) Segmento de Internos y Control.

| **Segmento de Internos y Control** | | | | **☑ Obligatorio ☑ Único** |
|---|---|---|---|---|
| **SICRES 4.0** | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Identificador de Intercambio. | Alfanumérico. | 33 | Obligatorio. | Identificador de Intercambio único de la operación. Se compondrá siguiendo la normalización definida en el Anexo 1 A. |
| Tipo de transporte de entrada. | Alfanumérico. | 2 | Opcional. | Formas de llegada al registro de entrada:<br>– '01' = Servicio de Mensajeros.<br>– '02' = Correo postal.<br>– '03' = Correo postal certificado.<br>– '04' = Burofax.<br>– '05' = En mano.<br>– '06' = Fax.<br>– '07' = Otros.<br>– '08' = Otros medios electrónicos. |
| Número de transporte de entrada. | Alfanumérico. | 40 | Opcional. | Referencia del transporte. Código. En el caso de certificados, número del mismo. |
| Nombre de usuario. | Alfanumérico. | 80 | Opcional. | Nombre del usuario de Origen. |
| Contacto de usuario. | Alfanumérico. | 160 | Opcional. | Contacto del usuario de Origen (teléfono o dirección de correo electrónico). |
| Aplicación y versión emisora. | Alfanumérico. | 20 | Opcional. | Identifica la aplicación y su versión. |
| Tipo de Anotación. | Alfanumérico. | 2 | Obligatorio. | Indica el motivo de la anotación (siguiendo la normalización definida en el apartadoV.2). Los únicos valores posibles para el mensaje de datos de intercambio son:<br>– '01'= Pendiente (sin Identificador de Intercambio).<br>– '02' = Envío.<br>– '03' = Reenvío. |
| Descripción del Tipo de Anotación. | Alfanumérico. | 160 | Opcional. | |
| Documentación física y/o soportes. | Número. | 1 | Obligatorio. | Indica si el fichero va acompañado de documentación física.<br>– '1' = Acompaña documentación física (u otros soportes) requerida.<br>– '2' = Acompaña documentación física (u otros soportes) complementaria.<br>– '3' = No acompaña documentación física ni otros soportes. |
| Observaciones del apunte. | Alfanumérico. | 160 | Opcional. | Observaciones del registro de datos de intercambio recogidos por el funcionario de registro. |
| Indicador de prueba. | Número. | 1 | Opcional. | Indica si el asiento registral es una prueba.<br>– '0' = Normal.<br>– '1' = Prueba. |

| Segmento de Internos y Control | | | | ☑ Obligatorio<br>☑ Único |
|---|---|---|---|---|
| SICRES 4.0 | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Identificador de intercambio previo. | Alfanumérico. | 33 | Opcional. | En caso de que el intercambio registral se trate de una rectificación de un intercambio previo, es decir, se trate de un envío como consecuencia de haber confirmado por error un registro recibido, este campo permitirá vincular este intercambio registral con el previo. |
| Código Entidad Registral de Inicio. | Alfanumérico. | 21 | Obligatorio. | Código único de la Entidad Registral de Inicio obtenido de Directorios Unificados indicados en el apartado VI.4. |
| Decodificación Entidad Registral de Inicio. | Alfanumérico. | 120 | Opcional. | Descripción de la Entidad Registral de Inicio. |
| Código de la Unidad de Tramitación de Inicio. | Alfanumérico. | 21 | Opcional. | Código único obtenido de Directorios Unificados indicados en el apartado VI.4. |
| Decodificación de la Unidad de Tramitación de Inicio. | Alfanumérico. | 120 | Opcional. | Descripción de la Unidad de Tramitación Inicio. |

Tabla 6. Datos de Internos y Control

Las consideraciones a tener en cuenta para asignar valor al campo ‘Documentación física y/o soportes’ son:

i. Acompaña documentación física (u otros soportes) requerida (‘1’). Indica que el mensaje de datos de intercambio debe ser tratado junto con documentación física (u otros soportes) necesaria para su trámite. Por tanto, no se puede aceptar y reenviar (si aplica) el fichero de intercambio hasta que toda la documentación física requerida haya sido recibida en la Entidad Registral de destino. Tampoco se puede dar número de registro oficial a la entrada, dándole temporalmente el tratamiento de ‘pre-asiento’, hasta disponer de la documentación física requerida.

Ejemplo de este caso, sería un intercambio en el que se realiza copia electrónica auténtica sólo de una parte de los documentos presentados, o cuando dichas copias no se pueden realizar (no se dispone de medios o el soporte no permite la digitalización correcta, como en el caso de sobres cerrados).

ii. Acompaña documentación física (u otros soportes) complementaria (‘2’). Indica que se envía documentación física (u otros soportes) que acompaña al mensaje de datos de intercambio, pero que ésta no es estrictamente necesaria para su trámite. Por tanto, se podría aceptar, pero no se podría reenviar (si aplica) el fichero de intercambio hasta que toda la documentación física haya sido recibida en la Entidad Registral de destino.

iii. No acompaña documentación física ni otros soportes (‘3’). Indica que el mensaje de datos de intercambio no se acompaña de ninguna documentación física ni otros soportes. Por tanto, se podría aceptar y reenviar (si aplica) el fichero de intercambio en cuanto llegue a la Entidad Registral de destino.

Además, este segmento incorpora la posibilidad de incluir información sobre la Entidad Registral de Inicio, cuya localización es necesaria para que un mensaje de datos de intercambio, que ha sido rechazado, pueda ser reenviado a la Entidad Registral que originó el proceso de intercambio, sin perder el rastro de la Entidad Registral que generó el reenvío. El modo en que el mensaje de datos de intercambio es reenviado a la Entidad Registral de Inicio se desarrolla en el apartado V de esta norma.

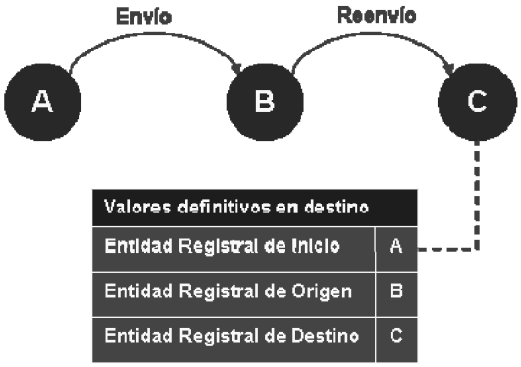



**Figura 3.** Diferenciación Entidad Registral de Inicio - Entidad Registral de Origen

Del mismo modo, el segmento incorpora también la posibilidad de incluir información sobre la Unidad de Tramitación de Inicio.

G) Segmento de Formulario Genérico.

| Segmento de Formulario Genérico | | | | ☑ Opcional<br>☑ Único |
|---|---|---|---|---|
| SICRES 4.0 | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Expone. | Alfanumérico. | 4000 | Obligatorio. | Exposición de los hechos y antecedentes relacionados con la solicitud. |
| Solicita. | Alfanumérico. | 4000 | Obligatorio. | Descripción del objeto de la solicitud. |

Tabla 7. Datos de Formulario Genérico

Este segmento opcional permite el intercambio del contenido de los formularios de propósito general que se implementan en los registros electrónicos.

Si se utiliza, además de incluir los datos específicos de este segmento, el formulario genérico se deberá incluir como documento anexo en el segmento de Anexo.

Esto permite que se puedan intercambiar formularios genéricos tanto con registros electrónicos con registros presenciales.

IV.3 Estructura y contenido del mensaje de control.

La entidad mensaje de control en SICRES 4.0 es un fichero que contiene la información de control y notificación acerca del estado de una operación de intercambio.

A continuación se definen los campos que componen un mensaje de control a utilizar, no así, el formato en que se implementen dentro del sistema de gestión de intercambio.

| Segmento de Mensaje de Control | | | | ☑ Obligatorio<br>☑ Único |
|---|---|---|---|---|
| SICRES 4.0 | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Código Entidad Registral de Origen. | Alfanumérico. | 21 | Obligatorio. | Código único obtenido de Directorios Unificados indicados en el apartado VI.4. |
| Código Entidad Registral de Destino. | Alfanumérico. | 21 | Obligatorio. | Código único obtenido de Directorios Unificados indicados en el apartado VI.4. |
| Identificador de Intercambio. | Alfanumérico. | 33 | Obligatorio. | Identificador de Intercambio único de la operación. Se compondrá siguiendo la normalización definida en el Anexo 1A. |
| Tipo de mensaje. | Alfanumérico. | 2 | Obligatorio. | Indica el tipo de mensaje (siguiendo la normalización definida en el apartado V.3). Los valores que el tipo de mensaje de control puede tomar son:<br>– '01' = ACK (aceptación).<br>– '02' = Error.<br>– '03' = Confirmación.<br>– '04' = ACK a Confirmación.<br>– '05' = Rechazo.<br>– '06' = ACK a Rechazo. |
| Descripción del mensaje. | Alfanumérico. | 1024 | Opcional. | Texto descriptivo del mensaje de control. |
| Número de registro de entrada en destino. | Alfanumérico. | 20 | Opcional. | Número de registro de entrada en la Entidad Registral destino. Utilizado para completar el ciclo de envío. |
| Fecha y hora de entrada en destino. | Alfanumérico. | 19 | Opcional. | Formato AAAAMMDDHHMMSSZ. |

| Segmento de Mensaje de Control | | | | ☑ Obligatorio<br>☑ Único |
|---|---|---|---|---|
| SICRES 4.0 | | | | |
| **Descripción** | **Tipo** | **Longitud** | **Obligación** | **Comentarios** |
| Indicador de prueba. | Número. | 1 | Obligatorio. | Indica si el mensaje es una prueba.<br>– '0' =Normal.<br>– '1' =Prueba. |
| Identificador de fichero. | Alfanumérico. | 50 | Opcional. | Identificador del mensaje de datos que se tiene que reenviar en caso de error. Se compondrá siguiendo la normalización definida en el Anexo 1 B, con tipo de fichero = '01' (anexo).<br>Es opcional y múltiple, dado que el error puede producirse durante el envío de cualquiera de los ficheros: mensaje de datos de intercambio y Anexos (opcionales y múltiples). |
| Código de error. | Alfanumérico. | 4 | Opcional. | Identifica el tipo de error que se ha producido durante el envío del mensaje de datos de intercambio.<br>Se compondrá siguiendo la normalización definida en el Anexo 1.D.<br>Este valor sólo será aplicable en el caso de que el campo 'Tipo de Mensaje' tome el valor 'Error', codificado como '02'. |

Tabla 8. Datos de Mensaje de control

### *V. Descripción y estados del intercambio*

En este apartado se describen los posibles estados en los que se puede encontrar el apunte registral objeto del intercambio.

Tal y como se introdujo en el apartado IV.1, el proceso de intercambio inicia y finaliza en la Entidad Registral Origen, ya sea en el propio ciudadano o en la Unidad de Tramitación de Origen.

A lo largo de todo este proceso, Entidad Registral Origen y Destino se informan mutuamente sobre el estado del intercambio a través de sus respectivos campos:

i. Campo 'Tipo de anotación' del segmento de datos 'Internos y Control' del mensaje de datos de intercambio que emite la Entidad Registral Origen y destino.

ii. Campo 'Tipo de mensaje' de los mensajes de control que se envía.

De esta forma, el control sobre el estado del asiento registral a lo largo del proceso de intercambio se gestiona y controla de manera conjunta entre Origen y destino.

El inicio del intercambio viene marcado por la generación por parte de la Entidad Registral Origen del mensaje de datos de intercambio cuyo campo 'Tipo de anotación' tiene valor de *Pendiente.* El intercambio finaliza cuando, después de que la Entidad Registral de destino haya notificado a la Entidad Registral de Origen el asentimiento del intercambio enviándole un mensaje de control de tipo *confirmación,* esta Entidad Registral de Origen acepta el mensaje devolviéndole a la Entidad Registral de Destino un mensaje de control de tipo *ack.*

Las Entidades Registrales deben implementar mecanismos y procedimientos que eviten la duplicación de asientos en caso de recepciones múltiples. Las herramientas para esta implementación son los datos 'Identificador de Intercambio', 'Identificador de Fichero' y 'Número de Secuencia'.

V.1 Generación del Identificador de Intercambio.

La aplicación de registro de la Entidad Registral Origen que interviene en el proceso de intercambio, es responsable de la generación de un identificador de intercambio único para cada operación en el espacio de intercambio del tipo:

**<Código Entidad Registral Origen>_<AA>_<Número Secuencial>**

Este identificador se mantiene durante todo el proceso de intercambio tanto en el sistema de gestión de intercambio como en la aplicación de registro de la Entidad Registral destino. En el apartado Anexo 1A se describen las reglas para la generación de este identificador.

V.2 Estados en el mensaje de datos de intercambio.

Los estados que registra el mensaje de datos de intercambio en el campo de 'Tipo de anotación' son:

i. Pendiente ('01'): Indica que el mensaje de datos de intercambio está pendiente de envío al sistema de intercambio y que está pendiente de la asignación de un identificador del intercambio para iniciar el proceso.

ii. Envío ('02'): Indica que el mensaje de datos de intercambio está en pleno proceso de intercambio, y por tanto, ha partido desde la Entidad Registral de Origen pero está pendiente aún de convertirse en registro en firme por la Entidad Registral de destino.

iii. Reenvío ('03'): Indica que el mensaje de datos de intercambio es enviado de nuevo desde la Entidad Registral de destino.

La razón para el reenvío es, generalmente, que el destino indicado en el primer envío no corresponde. Cuando se da esta situación, la Entidad Registral de destino puede identificar la Entidad Registral de destino correcta y reenviarlo a ésta en lugar de rechazar el envío que realizó la Entidad Registral Origen.

Esta secuencia de envíos y los valores que toma el campo 'Tipo de anotación' aparecen en la siguiente figura.

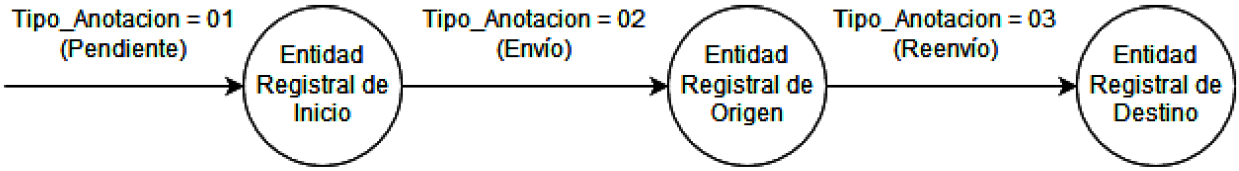



**Figura 4.** Tipo de anotación en mensaje de datos de intercambio en caso de reenvío

V.3 Estados en los mensajes de control.

La información de estado del intercambio que se refleja en los mensajes de control a través de los siguientes valores de 'Tipo de mensaje':

i. ACK-aceptación ('01'): Notifica la recepción correcta del mensaje de datos de intercambio desde un punto de vista exclusivamente técnico, por lo que no constituye la confirmación de finalización correcta de todo el proceso de intercambio.

A continuación, se muestra una figura explicativa de la emisión de un mensaje de control tipo aceptación:

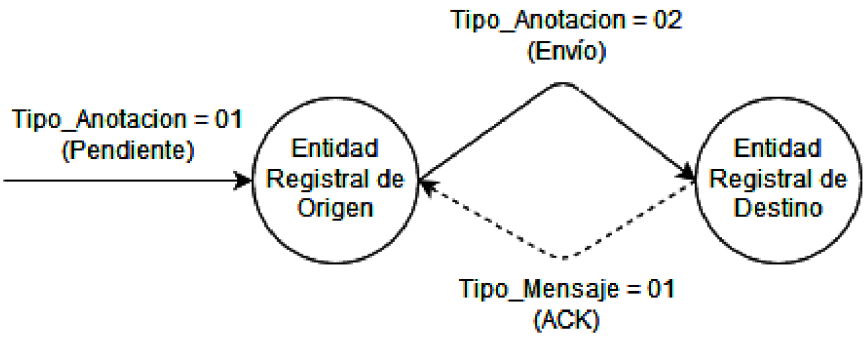



**Figura 5.** Emisión de mensaje de control ACK tras la recepción correcta del mensaje de datos de intercambio

Los mensajes de control de aceptación deberán emitirse también para notificar la recepción correcta desde el punto de vista técnico de los mensajes de control de tipo confirmación. En la figura 10 se muestra la emisión de este mensaje en tal escenario.

ii. Error ('02'): Notifica la recepción errónea o incompleta del mensaje de datos de intercambio desde un punto de vista técnico. Los posibles tipos de errores que se pueden dar se identifican mediante un rango de error y el propio código de error. Este mensaje de control refleja el tipo de error a través de la codificación de errores que se detalla en el Anexo 1.D.

La siguiente figura refleja la emisión de un mensaje de control tipo Error:

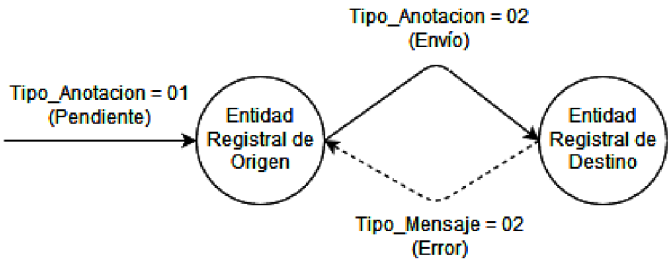



**Figura 6.** Emisión de mensaje de control tipo Error tras la recepción errónea del mensaje de datos de intercambio

Ante esta situación, la Entidad Registral de Origen ('A') puede enviar el mensaje de datos de intercambio a la Entidad Registral de destino ('B'), reenviarlo o rechazarlo.

iii. Confirmación ('03') y ACK Confirmación ('04'): Una vez recibido el mensaje de datos de intercambio y todos sus documentos anexos, se acepta que el proceso de intercambio se ha realizado con éxito y, por tanto, se notifica a la Entidad Registral de Origen o Inicio que la recepción ha sido correcta confirmando por tanto el asentimiento del intercambio completado.

La figura que sigue, muestra la secuencia que provoca la emisión de un mensaje de control tipo confirmación y la correspondiente aceptación de la confirmación:

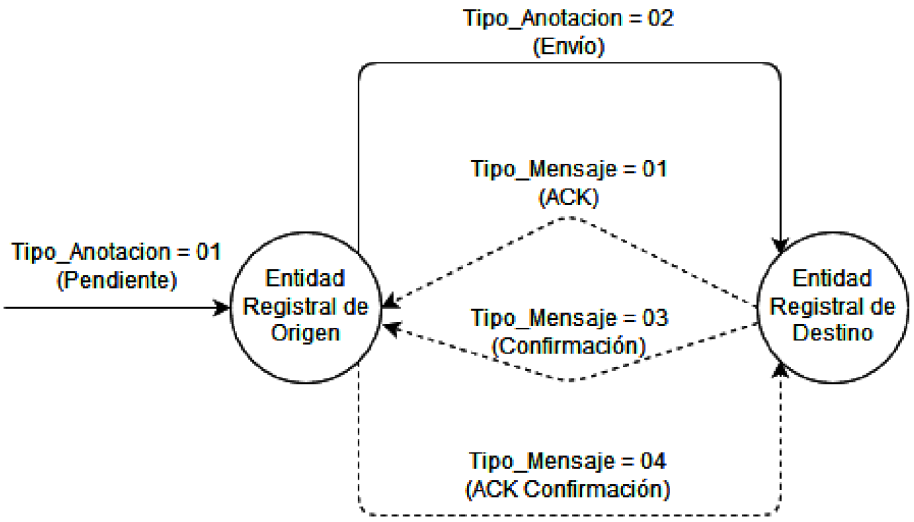



**Figura 7.** Envío de mensaje de control tipo Confirmación tras la recepción correcta del mensaje de datos de intercambio y sus anexos

El asentimiento es necesario para el correcto funcionamiento de los flujos de intercambio definidos, por lo que debe ser implementado por todas las Entidades Registrales para el intercambio de los asientos. El asentimiento permite confirmar que el asiento registral es correcto y corresponde a la Entidad Registral de destino por lo que debe emitirse tanto tras la recepción de un mensaje de datos de intercambio con 'Tipo de anotación' envío como si se trata de un *reenvío*.

La Entidad Registral de Destino deberá reenviar el Mensaje de Control de confirmación si pasado un periodo de tiempo (predefinido en cada sistema de intercambio) no recibe de la Entidad Registral de Origen o Inicio el Mensaje de Control de *ACK Confirmación.*

iv. Rechazo ('05') y ACK Rechazo ('06'): Indica que el mensaje de datos de intercambio no ha sido aceptado por la Entidad Registral de destino.

En caso de rechazo, el mensaje de datos de intercambio será enviado siempre a la Entidad Registral de Inicio.

La Entidad Registral de Destino deberá reenviar el Mensaje de Control de rechazo si pasado un periodo de tiempo (predefinido en cada sistema de intercambio) no recibe de la Entidad Registral de Inicio el Mensaje de Control de ACK Rechazo.

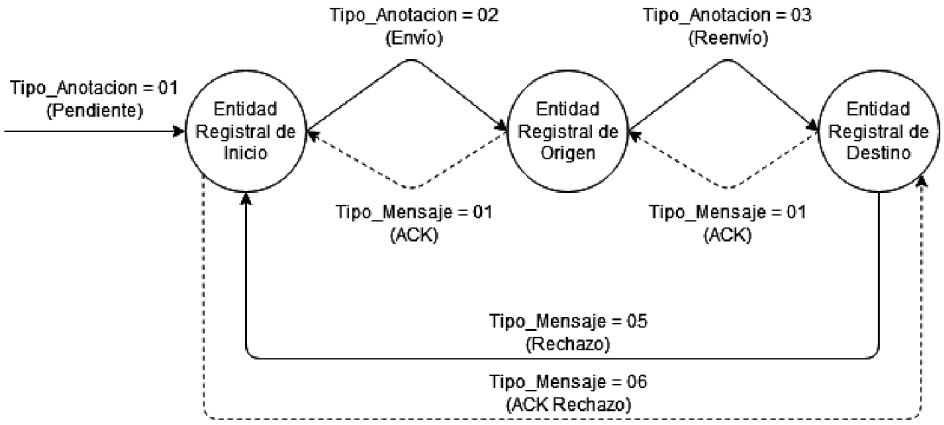



**Figura 8.** Tipo de anotación en mensaje de datos de intercambio en caso de rechazo

***VI. Funciones y requisitos del sistema de intercambio.***

El sistema de intercambio utilizado para emisión y recepción de los mensajes definidos en los apartados anteriores funciona, en el espacio de intercambio SICRES, como elemento responsable de:

i. Centralizar el registro de operaciones de intercambio y garantizar la trazabilidad de las mismas.
ii. Gestionar la situación temporal de los 'pre-asientos registrales'.
iii. Proporcionar la seguridad en el transporte de la información a través de mecanismos de encriptación en el mensaje de datos de intercambio.
iv. Firma electrónica del mensaje de datos de intercambio.

Como ya se ha indicado, esta norma no establece los requisitos tecnológicos concretos que deben proporcionar el sistema que da soporte a un intercambio de asientos registrales, ya que SICRES4.0 es independiente de la tecnología o plataforma sobre la que se realice la transmisión de los elementos que forman el intercambio propiamente dicho.
No obstante, sí se establecen unos principios básicos que deben ser cubiertos por el sistema de intercambio que se utilice, como son:

i. Integridad: Garantía de que la información no es modificada en los procesos de intercambio.
ii. Confidencialidad: Disponibilidad de la información solamente para usuarios autorizados.
iii. Autenticidad: Legitimidad del origen de la información.
iv. No repudio: Imposibilidad de negación ante terceros del envío y/o recepción por parte del emisor y/o receptor de la información.
v. Accesibilidad: Posibilidad de acceso eficiente sólo para entidades autorizadas.

A continuación se desarrollan estos requisitos de seguridad y, posteriormente, las funciones que debe proporcionar el sistema de intercambio.

VI.1 Requisitos de seguridad.

a) Autenticación de los sistemas implicados.

Además de la implementación de las políticas de seguridad para los usuarios de la plataforma de intercambio, se asegura la identidad de cada uno de los sistemas intervinientes en el espacio de intercambio.
Así, todos los sistemas que participen en el proceso de intercambio, incluidos los sistemas de las Entidades Registrales de Origen y Destino, están correctamente identificados y validados en el espacio de intercambio.

b) Integridad.

La plataforma de intercambio proporciona los mecanismos necesarios, a fin de garantizar que el contenido completo de los mensajes de datos intercambiados permanezca inalterado durante el proceso de intercambio.

Este punto se asegura a través del protocolo de transporte de mensajes entre las Entidades Registrales de Origen y Destino que utilice el sistema de intercambio, y la tecnología de transmisión de datos.

c) Garantía de no repudio.

La plataforma de intercambio provee de los mecanismos necesarios para garantizar el no repudio del mensaje de datos de intercambio.

VI.2 Gestión del proceso de intercambio.

Como ya se ha mencionado, para iniciar el intercambio, la aplicación de registro de la Entidad Registral Origen genera el mensaje de datos de intercambio de forma completa y lo envía al sistema de gestión de intercambio.

La plataforma de intercambio es responsable de verificar la validez del mensaje de datos de intercambio según el formato establecido en esta norma.

Además, el sistema de gestión de intercambio es el encargado de garantizar la transmisión entre los sistemas de la Entidad Registral Origen y destino.

Posteriormente, la aplicación de registro de la Entidad Registral destino es la responsable de interpretar de forma correcta el fichero intercambiado.

Hasta que el intercambio concluye, la plataforma de intercambio tiene la misión de resolver de forma correcta la situación temporal del ‘pre-asiento registral’ que desaparece cuando se produce la recepción completa de todos los ficheros que pudieran constituir un envío.

Dentro de cada espacio de intercambio debe definirse un conjunto de reglas que permitan la gestión del intercambio entre Entidades Registrales a través de un sistema de intercambio. Estas reglas permiten definir los mecanismos y herramientas para realizar el intercambio en condiciones adecuadas incluyendo:

i. La tecnología de comunicación entre los distintos agentes del intercambio.

ii. Los mecanismos y procedimientos específicos para el envío y recepción de ficheros, y para garantizar la integridad y seguridad de los envíos.

iii. Las políticas específicas de protección de datos que deben ser de aplicación.

iv. Los mecanismos de trazabilidad de los intercambios y la información que se registre sobre los mismos.

v. Procedimientos detallados de gestión de errores y excepciones.

a) Gestión de envíos de mensajes y anexos.

La plataforma de intercambio debe realizar una gestión adecuada del envío de mensajes y los posibles documentos anexos asociados, que garantice la correcta identificación del registro completo en la Entidad Registral de destino y su posterior almacenamiento.

b) Gestión del flujo.

Las operaciones de intercambio tienen definido un estado (definidos en el apartado V de la presente norma) en el que se indica la fase lógica dentro del proceso de intercambio en la que se encuentra el fichero, y los posibles eventos que pueden ocurrir.

c) Evitar duplicados.

El sistema de gestión de intercambio contiene los mecanismos necesarios para garantizar que los asientos que se envíen o reciban por duplicado de manera errónea, sean identificados como tales.

Las Entidades Registrales deben implementar mecanismos y procedimientos que eviten la duplicación de asientos en caso de que se reciban varias veces, utilizando los datos ‘Identificador de Intercambio’, ‘Identificador de Fichero’ y ‘Número de Secuencia’.

d) Gestión de mensajes.

El sistema de intercambio dispone de funcionalidades de gestión de mensajes de actividad, a fin de proporcionar información de seguimiento a la Entidad Registral de Origen, una vez realizado el intercambio, tal y como se describe en el apartado V.

La gestión y conservación de los anexos, entendidos éstos como documentos electrónicos, se definen y normalizan en la *NTI de Política de gestión de documentos electrónicos.*

e) Conservación de la información del asiento registral.

Cuando los pre-asientos registrales intercambiados no se convierten en asientos firmes en la Entidad Registral de destino, ésta no debe conservar el mensaje de datos de intercambio ni sus documentos adjuntos. Únicamente debe conservar traza de la transacción de intercambio realizada.

VI.3 Soporte del modo de prueba.

El sistema de gestión de intercambio debe disponer de la capacidad de soportar el modo de prueba en el proceso de intercambio, de tal forma que permita realizar pruebas de intercambio.

El modelo de datos incluye un identificador para mensajes de datos de intercambio que indica que son una prueba que aparece detallado en los apartados IV.2 y IV.3.

VI.4 Directorios unificados de organismos, entidades y unidades.

En el sistema de intercambio se deberán emplear códigos de identificación unívoca de las Entidades Registrales y Unidades de Tramitación que actúan como emisoras o receptoras de asientos registrales (campos de Entidades Registrales y Unidades de Tramitación de los segmentos «De Origen», «De Destino» y «De internos y control»). Para ello, podrán emplearse los siguientes directorios unificados:

i. Directorio Común de Unidades Orgánicas y Oficinas (DIR3): directorio que, cumpliendo con el artículo 9 del Real Decreto 4/2010, codifica de forma unívoca, tanto los organismos, órganos y unidades de tramitación de las administraciones públicas, como las Oficinas de Registro y atención al ciudadano, y mantiene información sobre ellos y las relaciones entre ellos.

ii. Directorio de Entidades (DIRe): directorio que mantiene información sobre personas jurídicas del ámbito privado y su estructura organizativa, asignando códigos de identificación unívoca a las posibles unidades de tal estructura.

iii. Otros directorios unificados que puedan crear y acordar las administraciones públicas.

Los códigos de estos directorios podrán también ser empleados para identificar y facilitar la obtención de información complementaria o adicional sobre los interesados (campo «Código de Directorios unificados» del «Segmento de Interesado»).

VI.5 Control y gestión de errores.

La plataforma de intercambio es responsable de realizar una gestión adecuada de los errores y excepciones que puedan ocurrir durante el proceso de intercambio, que facilite la restauración de información en la medida de lo posible.

a) Tipología de errores de intercambio.

Los principales errores que pueden ocurrir durante el intercambio registral pueden clasificarse, en base a la naturaleza del error, como:

i. Errores lógicos: relativos a errores en las validaciones en estructura y/o en contenido de los ficheros de intercambio y/o en direcciones de origen o destino. En definitiva, cualquier error no achacable a un problema tecnológico, pero que provoca que el resultado del intercambio no sea exitoso.

ii. Errores físicos: relativos a errores que se pueden asociar con la tecnología que interviene en el proceso de intercambio, como la no disponibilidad de máquinas, de elementos de la infraestructura de software, excepciones de código no controladas y otros.

iii. Errores de transmisión de datos: relativos a errores que pueden ocurrir durante la transmisión de datos debido a problemas en las comunicaciones.

La codificación de los errores aparece en el Anexo 1.D.

| Tipo de error | | Definición |
|---|---|---|
| Errores lógicos. | Errores de validación de los datos de intercambio. | Ocurren al resultar erróneas las validaciones lógicas de los datos del intercambio en formatos, datos requeridos y correspondencia entre descripciones de contenido y el contenido de los datos de intercambio. |
| | Errores de direccionamiento. | Ocurren cuando la identidad del remitente o destinatario reflejada en el mensaje de datos de intercambio no se corresponde con el que debería enviar o recibir la información. |
| | Errores en las reglas de intercambio. | Aparece un evento no esperado durante el intercambio registral. |
| | Errores de ciclo de envío no completado. | No se puede completar el ciclo de envío completamente. |
| Errores físicos. | | Se producen cuando ocurren errores, hardware o software, en alguno de los sistemas intervinientes. |
| Errores de transmisión de datos. | | No se puede producir el intercambio, debido a que el sistema de destino o el de Origen no están disponibles. |

Tabla 9. Descripción de errores de intercambio

b) Errores lógicos.

Descripción de los errores lógicos:

i. Errores de validación de los datos de intercambio. Ocurren al resultar erróneas las validaciones lógicas de los datos del intercambio en formatos, datos requeridos y correspondencia entre descripciones de contenido y el contenido de los datos de intercambio.

ii. Errores de direccionamiento. Ocurren cuando la identidad del remitente o destinatario reflejada en el mensaje de datos de intercambio no se corresponde con el que debería enviar o recibir la información.

iii. Errores en las reglas de intercambio. Aparece un evento no esperado durante el intercambio registral.

iv. Errores de ciclo de envío no completado. No se puede completar el ciclo de envío completamente.

Tratamiento de los errores lógicos:

i. Errores de validación de los datos de intercambio. En el momento que se detecte esta falta de integridad en los datos de intercambio, se deberá interrumpir el proceso marcando como erróneo el mensaje de datos de intercambio. A continuación se deberá notificar al Origen de que no se ha podido interpretar correctamente los datos, informándole del código de error lógico ocurrido.

Una vez notificado, la Entidad Registral de Origen se dispondrá a analizar la naturaleza del error para realizar acciones de subsanación:

1. Si es relativo a una composición errónea del mensaje de datos de intercambio y anexos asociados, deberá recomponerlos y retransmitirlos.
2. Si el error es debido a una corrupción de datos durante la transmisión deberá simplemente retransmitirlos.

La operación deberá ser registrada como errónea en el log de operaciones del sistema de gestión del intercambio.

ii. Errores de direccionamiento. Se pueden producir por errores en la dirección del remitente o en el destinatario.

Si se produce un error en los datos del destinatario, es posible que sucedan dos escenarios:

1. Los datos llegan a una Entidad Registral de destino no esperada. En este caso, la Entidad destino deberá rechazar el registro recibido y notificar a la Entidad Origen de la ocurrencia de este suceso a través del sistema de gestión de intercambio.
2. Los datos llegan a un destino no esperado fuera del espacio de intercambio registral, es decir, no es enviado a una Entidad Registral. El error se podrá identificar por un aviso de error de direccionamiento proporcionado por el sistema de gestión de intercambio (por ejemplo ‘destino inalcanzable’), o al no recibirse la confirmación de la entrega pasado un tiempo preestablecido por parte de la Entidad Registral de Origen.

El tratamiento de estos errores se llevaría a cabo a través de la realización retransmisiones desde el sistema de intercambio o desde la Entidad Registral Origen, una vez solucionado el error de direcciones.

Si se produce un error en los datos del remitente, es posible que sucedan dos escenarios:

1. Se recibe una confirmación de entrega en una Entidad Registral de Origen no esperada. En este caso, la Entidad Origen deberá rechazar la confirmación.
2. La confirmación de entrega es enviada a una dirección fuera del espacio de nombres del intercambio registral. En este caso el error se detectará si la entidad Origen no recibe la confirmación de la entrega en un tiempo preestablecido o si al enviar la confirmación se produce un aviso de error de direccionamiento, por ejemplo 'destino inalcanzable'.

Para tratar los errores de destinatario se intentarán retransmisiones desde el sistema de intercambio o desde la Entidad Registral destino, una vez solucionado el error de direcciones.

Los errores de direcciones pueden estar motivados por entradas erróneas en el Directorio Común. En estos casos, se debe detectar (normalmente al aparecer errores de direccionamiento) y realizar la corrección de la entrada incorrecta.

Las operaciones anteriormente indicadas deberán ser registradas como erróneas en el log de operaciones del sistema de gestión de intercambio.

iii. Errores en las reglas de intercambio. Este error ocurrirá si aparece un evento no esperado durante el intercambio registral (por ejemplo, se recibe un segundo mensaje de control de confirmación de entrega correcta para un mismo Identificador de Intercambio).

En este caso, el sistema de gestión de intercambio se vuelve inconsistente, por lo que se deberá registrar el elemento que ha producido el evento, y realizar una notificación para solucionar el problema.

iv. Errores de ciclo de envío no completado. Este error ocurrirá si no se hubiera podido cerrar el ciclo de envío completo, al interrumpirse en alguno de sus pasos. Se detecta al sobre pasarse los límites de tiempo esperados para que un paso del ciclo se realice.

El Origen de este error puede ser variado, debido tanto a problemas lógicos como físicos. El tratamiento normal para estos casos es la retransmisión de los datos.

La operación errónea deberá ser registrada en el log del sistema de gestión de intercambio, indicando los reintentos efectuados y si fueron exitosos o no. Si al efectuar el número de reintentos determinado no se consiguiera cerrar el ciclo, el conjunto de datos objeto del error deberá ser marcado como erróneo notificando a el sistema de intercambio, la necesidad de un tratamiento para su subsanación.

c) Errores físicos.

Descripción de los errores físicos:

Se producen cuando ocurren errores, hardware o software, en alguno de los sistemas intervinientes.

Tratamiento de los errores físicos:

Los errores en el sistema de intercambio deben ser tratados según los procedimientos de operación que apliquen en cada caso.

Las operaciones de intercambio que se viesen afectadas por el error ocurrido se identificarán y restaurarán en la medida de lo posible.

d) Errores de transmisión.

Descripción de los errores de transmisión:

No se puede producir el intercambio, debido a que el sistema de destino o el de Origen no están disponibles.

Tratamiento de los errores de transmisión:

Si alguno de los sistemas no está disponible el tratamiento normal será la realización de reintentos de envío.

La operación errónea deberá ser registrada en el log del sistema de gestión de intercambio, indicando los reintentos efectuados y si fueron exitosos o no. Si al efectuar el número de reintentos establecidos no se consiguiera cerrar el ciclo, el conjunto de datos objeto del error deberá ser marcado como erróneo notificando al sistema de gestión de intercambio de la necesidad de un tratamiento para su subsanación.

### *VII. Otras recomendaciones*

Existen otros requerimientos de tecnología que pueden ser considerados como recomendaciones.

a) Registro de la actividad de intercambio.

Se recomienda, que el estado y la secuencia de las operaciones de intercambio se registren en un sistema centralizado del sistema de intercambio, que permita realizar la trazabilidad de las operaciones efectuadas.

Las aplicaciones de registro de las Entidades Registrales implicadas en un proceso de intercambio, podrán hacer uso de los datos de trazabilidad para proporcionar un servicio de seguimiento a los ciudadanos e instituciones que lo soliciten.

b) Persistencia en errores y excepciones.

Los datos del mensaje de datos de intercambio y el estado de sus operaciones a través del sistema de gestión de intercambio, deberían permanecer en un medio persistente cuando se produzcan errores o excepciones que impidan su envío/recepción. Se garantizará la perdurabilidad de registro y su estado, si ocurrieran errores en el proceso de intercambio.

## ANEXO 1

## Codificación

## ANEXO 1A

## Identificador del intercambio

A cada operación de intercambio se le asocia un identificador que permite designar la operación de forma única.

<Código Entidad Registral Origen>_<AA>_<Número Secuencial>

La codificación de este identificador se compone según el siguiente criterio:

| Campo | Definición / Valor |
|---|---|
| <Código Entidad Registral Origen>. | Código que figura para la Entidad Origen en Directorios Unificados indicados en el apartado IV.4, codificado en base a 21 caracteres. |
| <AA>. | Año en curso en dos dígitos. |
| <Número Secuencial>. | Con una longitud de 8 dígitos, suficiente para evitar que puedan repetirse dos Identificadores en la misma Entidad Registral. |

Tabla 10. Formato del identificador del intercambio

La generación de este código se realiza antes de enviar el Mensaje de datos de intercambio, al sistema de gestión de intercambio.

## ANEXO 1B

## Identificadores de ficheros de mensajes de datos de intercambio y anexos

En el proceso de intercambio se transmiten diferentes ficheros entre Origen y Destino. Por un lado, a través de la Plataforma de Intercambio, se transmiten ficheros con Mensajes de Datos de Intercambio y Mensajes de Control. Además, haciendo uso de las interfaces y

canales habilitadas por los repositorios del sistema de referencias únicas, se transmiten ficheros con documentos electrónicos en formato ENI que contiene los documentos anexos.

Todos estos ficheros deben ser intercambiados con nombres de acuerdo con un formato normalizado. El uso de esta notación permite identificar de forma única a los ficheros dentro del espacio de intercambio registral.

A continuación se muestra el formato del nombre que deben tener los ficheros de Mensajes de Datos de Intercambio y de fichero de Anexos:

<Identificador del Intercambio>_<Código de tipo de archivo>_<Número Secuencial>.<Extensión del fichero>

| Campo | Definición / Valor |
|---|---|
| <Identificador del Intercambio>. | Se genera tal y como se indica en el apartado anterior (Anexo 1 A).<br>Por tanto, este campo, a su vez, tendrá el formato:<br><Código Entidad Registral Origen>_<AA>_<Número Secuencial> |
| <Código de tipo de archivo>. | 00 = Mensaje SICRES: indica que el fichero es un mensaje de datos de intercambio.<br>01 = Anexo: indica que el fichero es un anexo. |
| <Número secuencial>. | Hasta cuatro dígitos y la secuencia puede reiniciarse con cada proceso de intercambio que tenga un identificador de intercambio diferente. |
| <Extensión del fichero>. | Formato que se determine para el intercambio. |

Tabla 11. Formato del identificador de los ficheros de Mensajes de Datos de Intercambio y de Anexos

## ANEXO 1C

### Identificador de ficheros de mensajes de control y notificación

Los ficheros de los Mensajes de Control se nombrarán de acuerdo con la siguiente estructura:

<Código de la Entidad Registral Emisora>_<AA>_<Número Secuencial>.>.<Extensión del fichero>

| Campo | Definición / Valor |
|---|---|
| <Código de la Entidad Registral Emisora>. | Código obtenido de Directorios Unificados indicados en el apartado IV.4 de la Entidad Registral que crea el mensaje, codificado en base a 21 caracteres. |
| <AA>. | Indica el año en curso, con una longitud de 2 dígitos. |
| <Número Secuencial>. | Con una longitud de 8 dígitos, suficiente para evitar que puedan repetirse dos identificadores en la misma Entidad Registral. |
| <Extensión del fichero>. | Formato que se determine para el intercambio. |

Tabla 12. Formato del Identificador de fichero del Mensaje de control y notificación

## ANEXO 1D

### Errores

Para realizar la codificación de los errores del sistema de intercambio, se utiliza un código de cuatro dígitos, estructurado en dos niveles:

i. Rango de error, que agrupa la definición de un tipo general de error. Se codifica con los dos primeros dígitos y establecen una secuencia:

**00**00
**01**00
**02**00
…
**99**00

ii. Código de error, pertenecientes a un rango. Utilizando los dos últimos dígitos, de la siguiente forma:

0000
0001
0002
…
0099

Por ejemplo, se puede definir un rango de error del tipo:

‘0000’ Errores en la validación del mensaje de datos de intercambio.

Y definir un error concreto como:

‘0001’ No se incorporan los anexos definidos en el mensaje de datos de intercambio.

## ANEXO 2

### Ejemplo esquema XML del modelo de datos SICRES 4.0

El objetivo de este anexo es mostrar el modelo de datos SICRES 4.0 en formato de esquema XML. Se adjuntarán ficheros XML de ejemplo.

Representación gráfica del esquema del mensaje de datos de intercambio

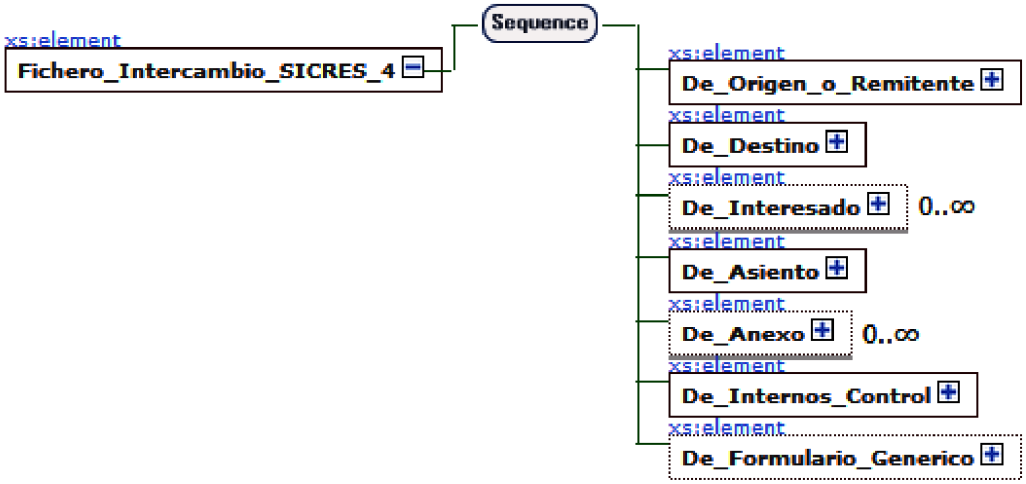



**Figura 9.** Esquema XML: Mensaje de datos de intercambio - Visión general

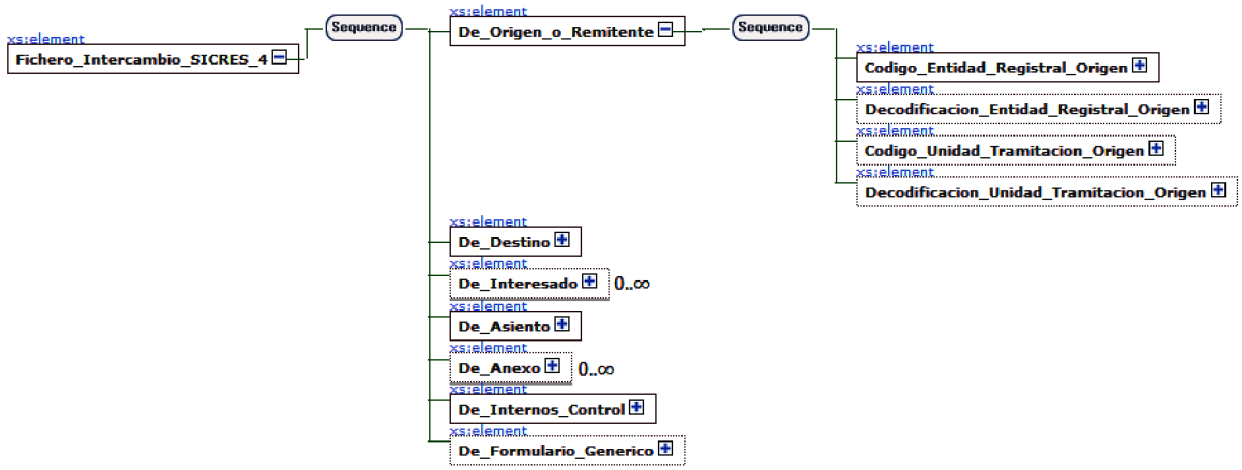



**Figura 10.** Esquema XML: Mensaje de datos de intercambio - Detalle de Origen o Remitente

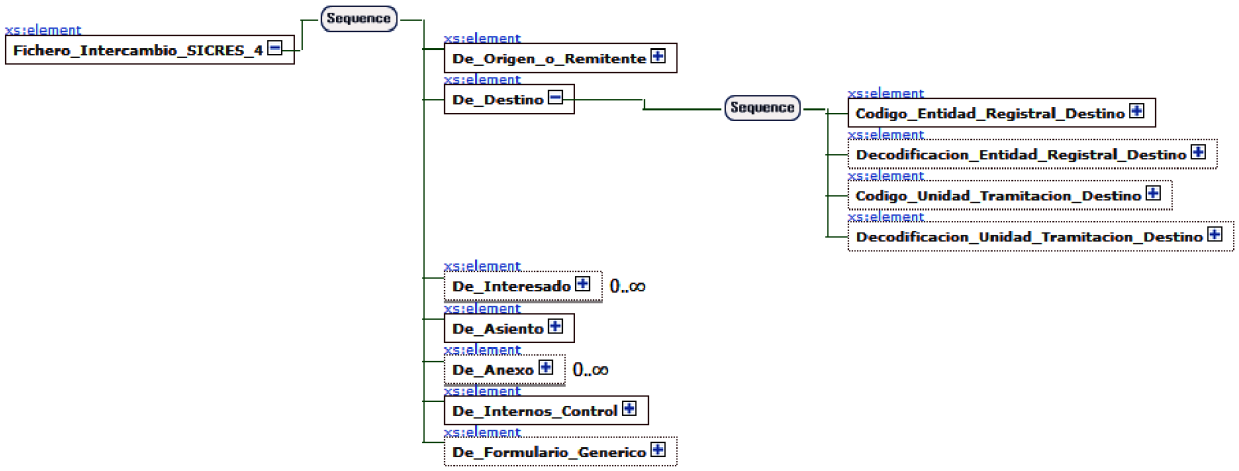



**Figura 11.** Esquema XML: Mensaje de datos de intercambio - Detalle de destino

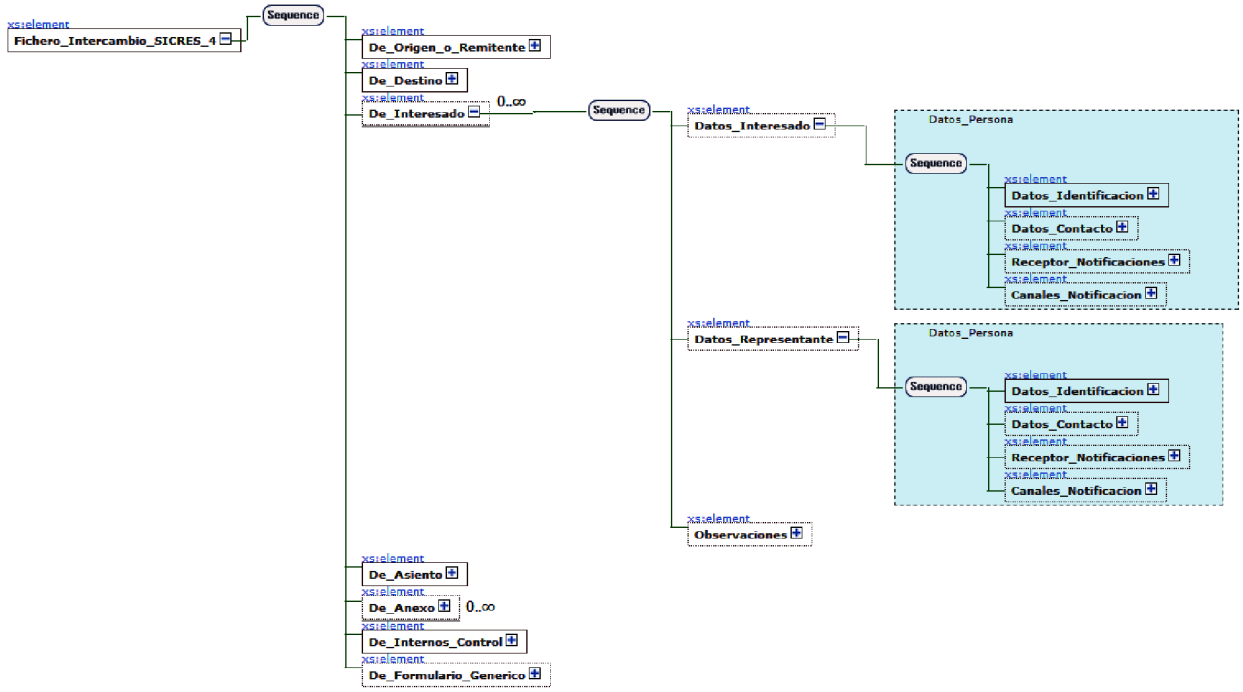



**Figura 12.** Esquema XML: Mensaje de datos de intercambio - Detalle de Interesado

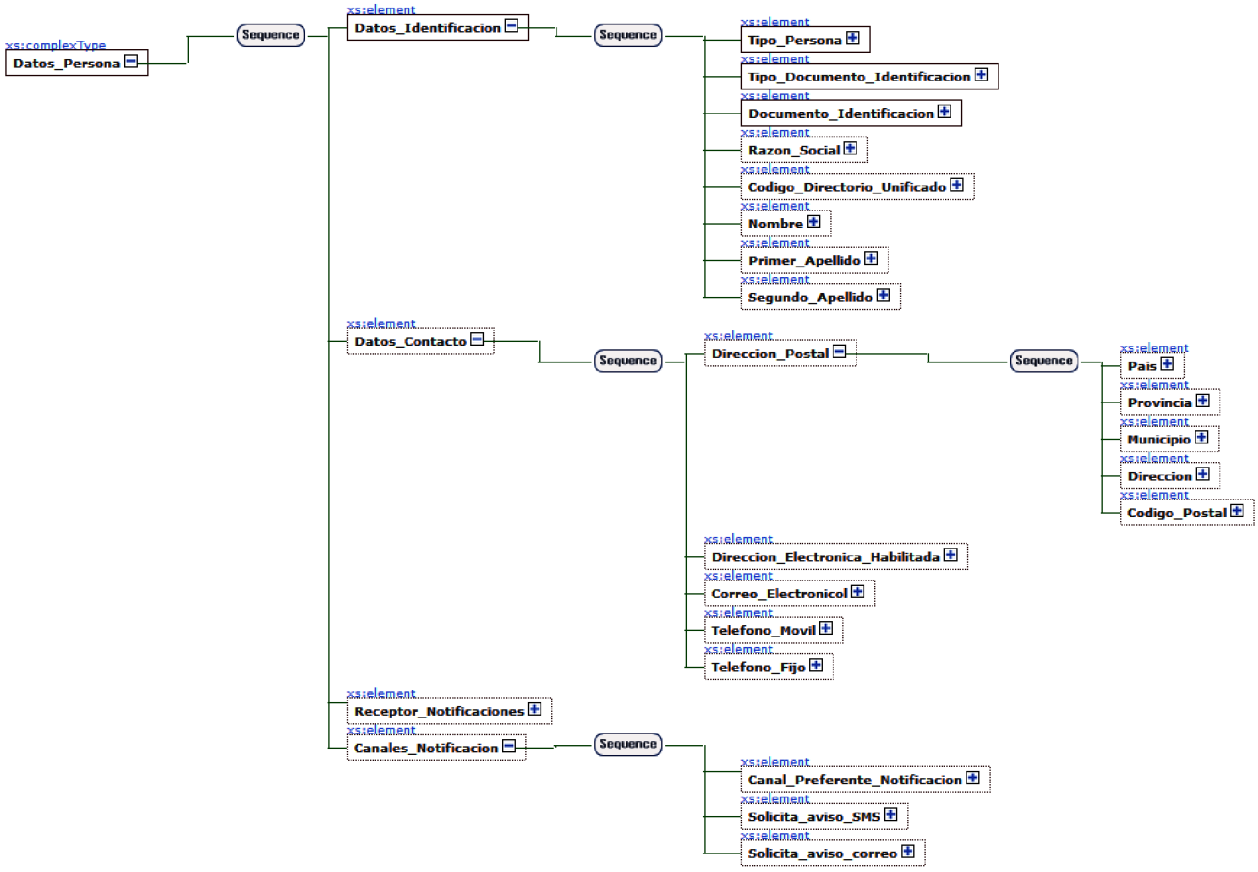



**Figura 13.** Esquema XML: Mensaje de datos de intercambio - Detalle de Datos de Persona

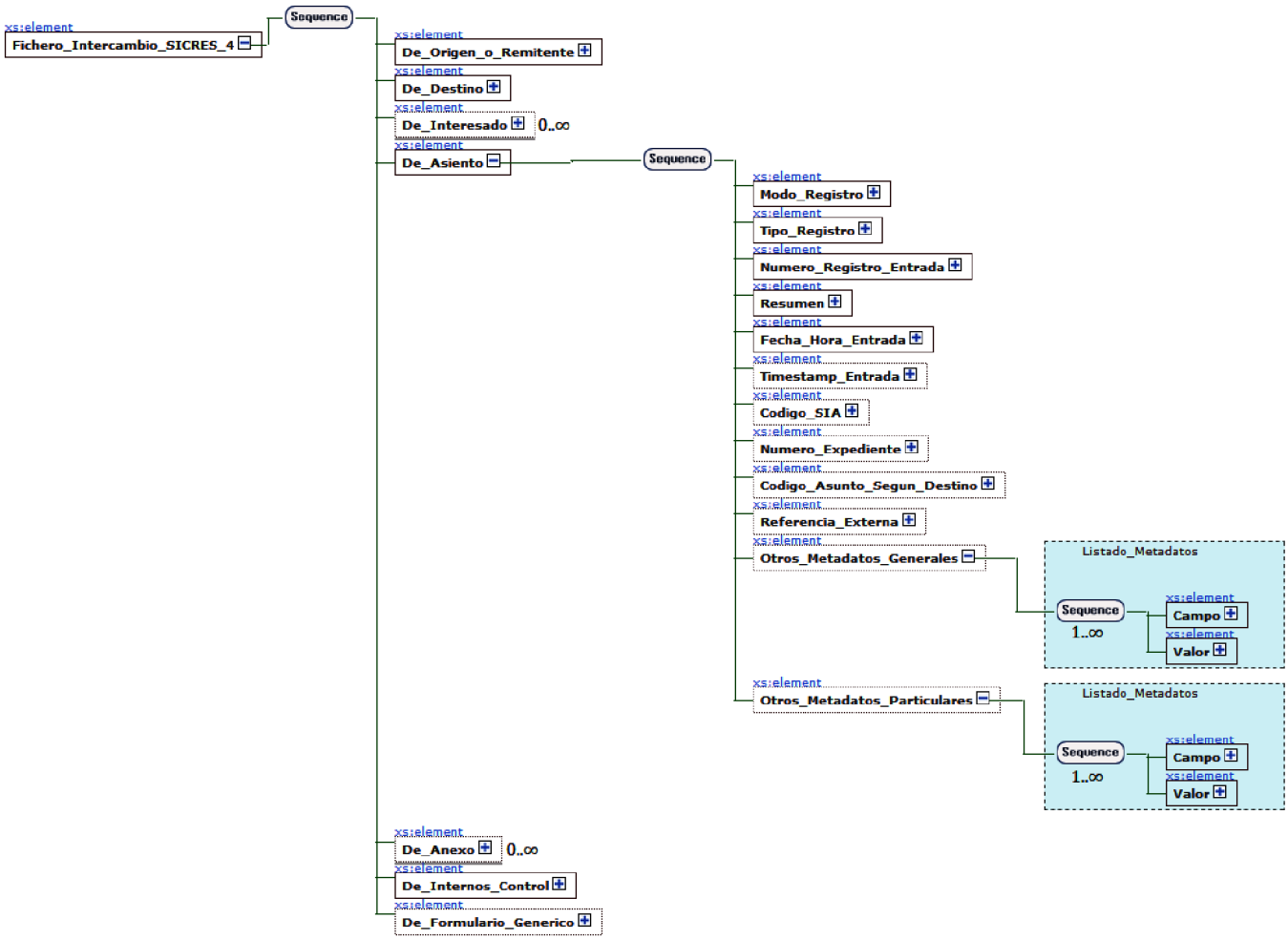



**Figura 14.** Esquema XML: Mensaje de datos de intercambio - Detalle de Asiento

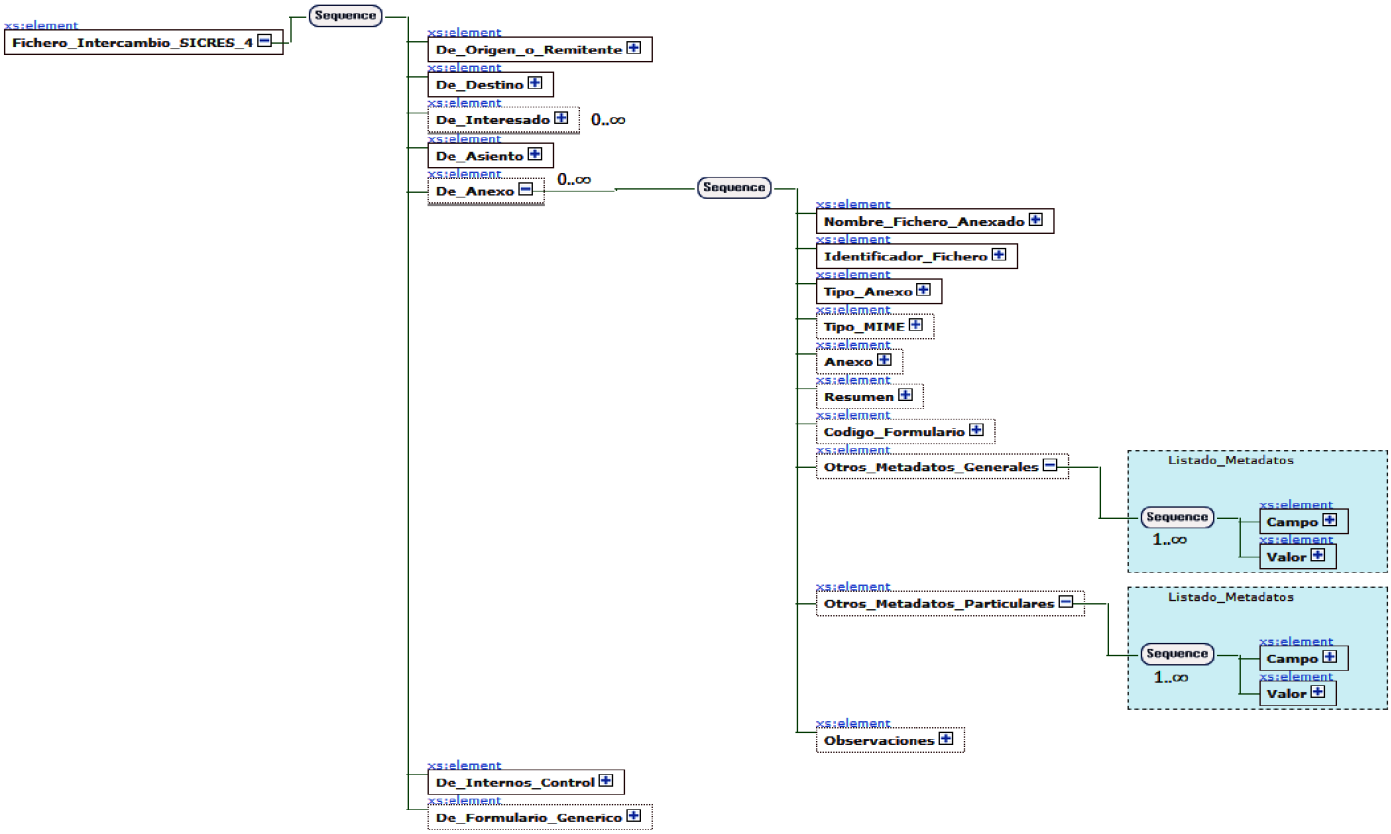



**Figura 15.** Esquema XML: Mensaje de datos de intercambio - Detalle de Anexo

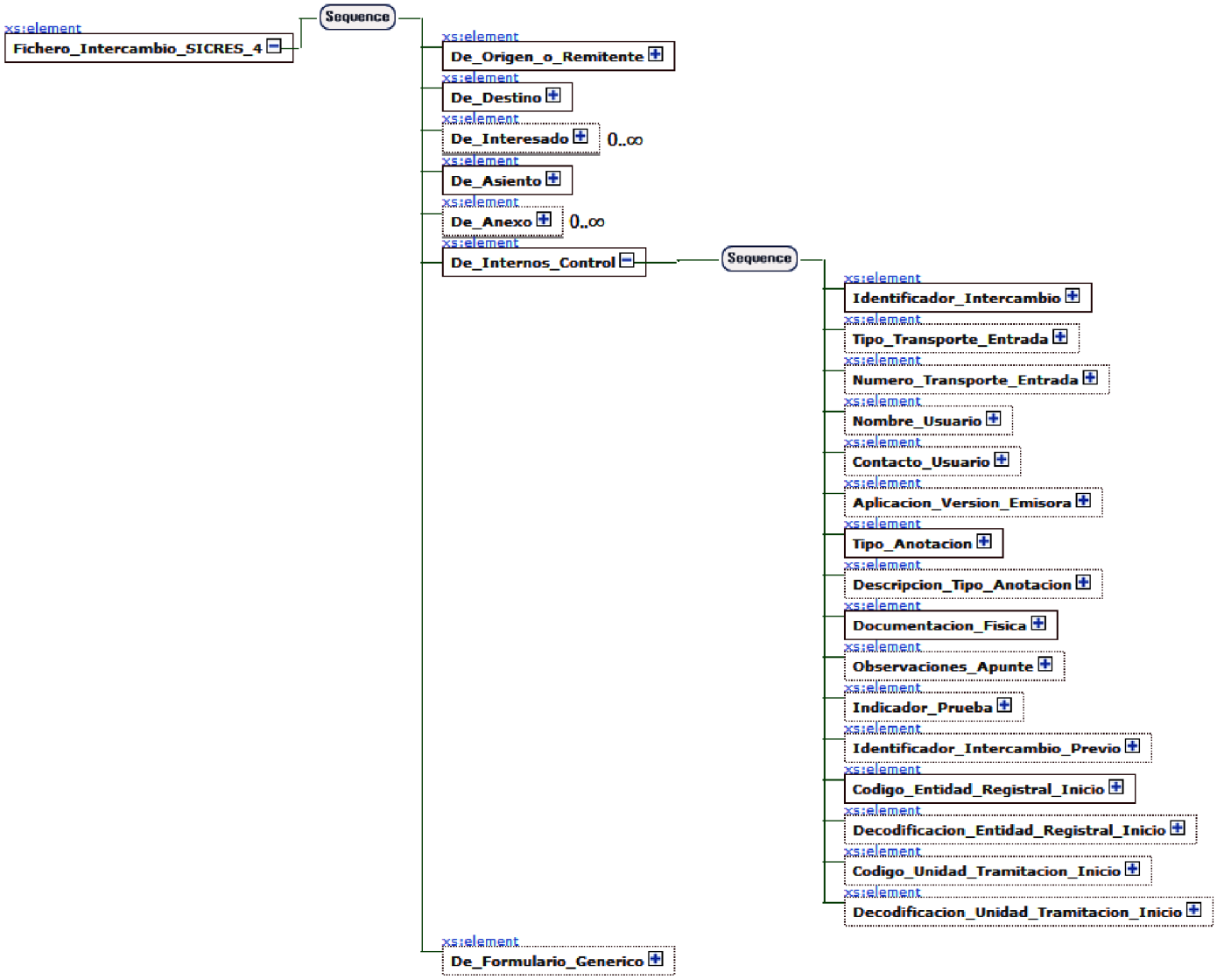



**Figura 16.** Esquema XML: Mensaje de datos de intercambio - Detalle de Internos y Control

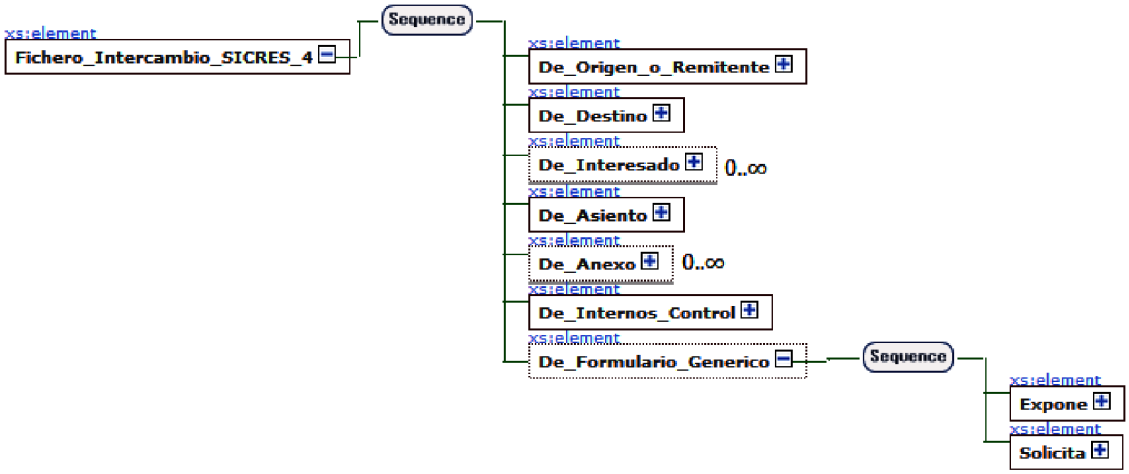



**Figura 17.** Esquema XML: Mensaje de datos de intercambio - Detalle de Formulario Genérico

Esquema XML del mensaje de datos de intercambio

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
	<!-- Declaracion de tipos complejos de ambito global -->
	<xs:complexType name="Datos_Persona">
		<xs:sequence>
			<xs:element name="Datos_Identificacion" minOccurs="1"
maxOccurs="1">
				<xs:complexType>
					<xs:sequence>
						<xs:element name="Tipo_Persona"
minOccurs="1" maxOccurs="1">
							<xs:simpleType>
								<xs:restriction base="xs:string">
									<xs:maxLength
value="1"/>
									<xs:enumeration
value="1"/>
									<xs:enumeration
value="2"/>
								</xs:restriction>
							</xs:simpleType>
						</xs:element>
						<xs:element
name="Tipo_Documento_Identificacion" minOccurs="1" maxOccurs="1">
							<xs:simpleType>
```

```
                                        <xs:restriction base="xs:string">
                                            <xs:maxLength
value="1"/>
                                            <xs:enumeration
value="N"/>
                                            <xs:enumeration
value="C"/>
                                            <xs:enumeration
value="P"/>
                                            <xs:enumeration
value="E"/>
                                            <xs:enumeration
value="X"/>
                                            <xs:enumeration
value="O"/>
                                        </xs:restriction>
                                    </xs:simpleType>
                                </xs:element>
                                <xs:element
name="Documento_Identificacion" minOccurs="1" maxOccurs="1">
                                    <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                            <xs:maxLength
value="17"/>
                                        </xs:restriction>
                                    </xs:simpleType>
                                </xs:element>
                                <xs:element          name="Razon_Social"
minOccurs="0" maxOccurs="1">
                                    <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                            <xs:maxLength
value="80"/>
                                        </xs:restriction>
                                    </xs:simpleType>
                                </xs:element>
                                <xs:element
name="Codigo_Directorio_Unificado" minOccurs="0" maxOccurs="1">
                                    <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                            <xs:maxLength
value="21"/>
                                        </xs:restriction>
```

```
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element  name="Nombre"  minOccurs="0"
maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="30"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element            name="Primer_Apellido"
minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="30"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element          name="Segundo_Apellido"
minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="30"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                </xs:sequence>
                            </xs:complexType>
                        </xs:element>
                        <xs:element          name="Datos_Contacto"          minOccurs="0"
maxOccurs="1">
                            <xs:complexType>
                                <xs:sequence>
                                    <xs:element            name="Direccion_Postal"
minOccurs="0" maxOccurs="1">
                                        <xs:complexType>
                                            <xs:sequence>
                                                <xs:element  name="Pais"
minOccurs="0" maxOccurs="1">
                                                    <xs:simpleType>
```

```
        <xs:restriction base="xs:string">
        <xs:maxLength value="4"/>
        </xs:restriction>
                                                    </xs:simpleType>
                                                </xs:element>
                                                <xs:element
name="Provincia" minOccurs="0" maxOccurs="1">
                                                    <xs:simpleType>
        <xs:restriction base="xs:string">
        <xs:maxLength value="2"/>
        </xs:restriction>
                                                    </xs:simpleType>
                                                </xs:element>
                                                <xs:element
name="Municipio" minOccurs="0" maxOccurs="1">
                                                    <xs:simpleType>
        <xs:restriction base="xs:string">
        <xs:maxLength value="5"/>
        </xs:restriction>
                                                    </xs:simpleType>
                                                </xs:element>
                                                <xs:element
name="Direccion" minOccurs="0" maxOccurs="1">
                                                    <xs:simpleType>
        <xs:restriction base="xs:string">
        <xs:maxLength value="160"/>
        </xs:restriction>
                                                    </xs:simpleType>
                                                </xs:element>
                                                <xs:element
name="Codigo_Postal" minOccurs="0" maxOccurs="1">
```

```
                                                    <xs:simpleType>
        <xs:restriction base="xs:string">
        <xs:maxLength value="5"/>
        </xs:restriction>
                                                    </xs:simpleType>
                                                </xs:element>
                                            </xs:sequence>
                                        </xs:complexType>
                                    </xs:element>
                                    <xs:element
name="Direccion_Electronica_Habilitada" minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="120"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element        name="Correo_Electronico"
minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="160"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element            name="Telefono_Movil"
minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="20"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element              name="Telefono_Fijo"
minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
```

```
                                                    <xs:maxLength
value="20"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                            <xs:element name="Receptor_Notificaciones" type="xs:boolean"
minOccurs="0" maxOccurs="1"/>
                            <xs:element name="Canales_Notificacion" minOccurs="0"
maxOccurs="1">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element
name="Canal_Preferente_Notificacion" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction base="xs:string">
                                                    <xs:maxLength
value="1"/>
                                                    <xs:enumeration
value="1"/>
                                                    <xs:enumeration
value="2"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element name="Solicita_aviso_SMS"
type="xs:boolean" minOccurs="0" maxOccurs="1"/>
                                        <xs:element name="Solicita_aviso_correo"
type="xs:boolean" minOccurs="0" maxOccurs="1"/>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                        </xs:sequence>
                    </xs:complexType>
                    <xs:complexType name="Listado_Metadatos">
                        <xs:sequence minOccurs="1" maxOccurs="unbounded">
                            <xs:element name="Campo">
                                <xs:simpleType>
                                    <xs:restriction base="xs:string">
                                        <xs:maxLength value="80"/>
                                    </xs:restriction>
```

```
                        </xs:simpleType>
                    </xs:element>
                    <xs:element name="Valor" type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <!-- Declaracion del elemento raiz del Mensaje de Datos de Intercambio SICRES --
>
            <xs:element name="Fichero_Intercambio_SICRES_4">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element                    name="De_Origen_o_Remitente"
minOccurs="1" maxOccurs="1">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element
name="Codigo_Entidad_Registral_Origen" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="21"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Decodificacion_Entidad_Registral_Origen" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="120"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Codigo_Unidad_Tramitacion_Origen" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="21"/>
                                                </xs:restriction>
                                            </xs:simpleType>
```

```
                                                    </xs:element>
                                                    <xs:element
name="Decodificacion_Unidad_Tramitacion_Origen" minOccurs="0" maxOccurs="1">
                                                        <xs:simpleType>
                                                            <xs:restriction
base="xs:string">
                                                                <xs:maxLength
value="120"/>
                                                            </xs:restriction>
                                                        </xs:simpleType>
                                                    </xs:element>
                                                </xs:sequence>
                                            </xs:complexType>
                                        </xs:element>
                                        <xs:element name="De_Destino" minOccurs="1"
maxOccurs="1">
                                            <xs:complexType>
                                                <xs:sequence>
                                                    <xs:element
name="Codigo_Entidad_Registral_Destino" minOccurs="1" maxOccurs="1">
                                                        <xs:simpleType>
                                                            <xs:restriction
base="xs:string">
                                                                <xs:maxLength
value="21"/>
                                                            </xs:restriction>
                                                        </xs:simpleType>
                                                    </xs:element>
                                                    <xs:element
name="Decodificacion_Entidad_Registral_Destino" minOccurs="0" maxOccurs="1">
                                                        <xs:simpleType>
                                                            <xs:restriction
base="xs:string">
                                                                <xs:maxLength
value="120"/>
                                                            </xs:restriction>
                                                        </xs:simpleType>
                                                    </xs:element>
                                                    <xs:element
name="Codigo_Unidad_Tramitacion_Destino" minOccurs="0" maxOccurs="1">
                                                        <xs:simpleType>
                                                            <xs:restriction
base="xs:string">
```

```
                                                    <xs:maxLength
value="21"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Decodificacion_Unidad_Tramitacion_Destino" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="120"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                            <xs:element      name="De_Interesado"      minOccurs="0"
maxOccurs="unbounded">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element  name="Datos_Interesado"
type="Datos_Persona" minOccurs="0" maxOccurs="1"/>
                                        <xs:element
name="Datos_Representante" type="Datos_Persona" minOccurs="0" maxOccurs="1"/>
                                        <xs:element      name="Observaciones"
minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="160"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                            <xs:element      name="De_Asiento"      minOccurs="1"
maxOccurs="1">
                                <xs:complexType>
                                    <xs:sequence>
```

```
                                        <xs:element      name="Modo_Registro"
minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="2"/>
                                                    <xs:enumeration
value="01"/>
                                                    <xs:enumeration
value="02"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element       name="Tipo_Registro"
minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="1"/>
                                                    <xs:enumeration
value="0"/>
                                                    <xs:enumeration
value="1"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Numero_Registro_Entrada" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="20"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element name="Resumen">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
```

```
value="240"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Fecha_Hora_Registro" minOccurs="1" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="19"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Timestamp_Registro" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
                                            <xs:element
name="Fecha_Hora_Presentacion" minOccurs="1" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="19"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Timestamp_Presentacion"          type="xs:base64Binary"          minOccurs="0"
maxOccurs="1"/>
                                            <xs:element          name="Codigo_SIA"
minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="80"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Numero_Expediente" minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
```

```
base="xs:string">
                                                    <xs:maxLength
value="80"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Codigo_Asunto_Segun_Destino" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="16"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Referencia_Externa" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="16"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Otros_Metadatos_Generales"      type="Listado_Metadatos"      minOccurs="0"
maxOccurs="1"/>
                                        <xs:element
name="Otros_Metadatos_Particulares"    type="Listado_Metadatos"    minOccurs="0"
maxOccurs="1"/>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                            <xs:element         name="De_Anexo"         minOccurs="0"
maxOccurs="unbounded">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element
name="Nombre_Fichero_Anexado" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
```

```
base="xs:string">
                                                    <xs:maxLength
value="80"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Identificador_Fichero" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="50"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element          name="Tipo_Anexo"
minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="2"/>
                                                    <xs:enumeration
value="01"/>
                                                    <xs:enumeration
value="02"/>
                                                    <xs:enumeration
value="03"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element          name="Tipo_MIME"
minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="80"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element                name="Anexo"
```

```
minOccurs="0" maxOccurs="1"/>
                                        <xs:element name="Resumen"
minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="160"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Codigo_Formulario" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="80"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Otros_Metadatos_Generales" type="Listado_Metadatos" minOccurs="0"
maxOccurs="1"/>
                                        <xs:element
name="Otros_Metadatos_Particulares" type="Listado_Metadatos" minOccurs="0"
maxOccurs="1"/>
                                        <xs:element name="Observaciones"
minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="160"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                            <xs:element name="De_Internos_Control" minOccurs="1"
maxOccurs="1">
                                <xs:complexType>
```

```
                                        <xs:sequence>
                                            <xs:element
name="Identificador_Intercambio" minOccurs="1" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="33"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Tipo_Transporte_Entrada" minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="2"/>
                                                        <xs:enumeration
value="01"/>
                                                        <xs:enumeration
value="02"/>
                                                        <xs:enumeration
value="03"/>
                                                        <xs:enumeration
value="04"/>
                                                        <xs:enumeration
value="05"/>
                                                        <xs:enumeration
value="06"/>
                                                        <xs:enumeration
value="07"/>
                                                        <xs:enumeration
value="08"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Numero_Transporte_Entrada" minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
```

```
value="40"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element   name="Nombre_Usuario"
minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="80"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element  name="Contacto_Usuario"
minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="160"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Aplicacion_Version_Emisora" minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="20"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element     name="Tipo_Anotacion"
minOccurs="1" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="2"/>
                                                        <xs:enumeration
value="01"/>
```

```
                                                    <xs:enumeration
value="02"/>
                                                    <xs:enumeration
value="03"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Descripcion_Tipo_Anotacion" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="160"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Documentacion_Fisica" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="1"/>
                                                    <xs:enumeration
value="1"/>
                                                    <xs:enumeration
value="2"/>
                                                    <xs:enumeration
value="3"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Observaciones_Apunte" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="160"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
```

```
                                        <xs:element  name="Indicador_Prueba"
minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="1"/>
                                                    <xs:enumeration
value="0"/>
                                                    <xs:enumeration
value="1"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Identificador_Intercambio_Previo" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="33"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Codigo_Entidad_Registral_Inicio" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="21"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Decodificacion_Entidad_Registral_Inicio" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="120"/>
                                                </xs:restriction>
                                            </xs:simpleType>
```

```
                                                    </xs:element>
                                                    <xs:element
name="Codigo_Unidad_Tramitacion_Inicio" minOccurs="0" maxOccurs="1">
                                                        <xs:simpleType>
                                                            <xs:restriction
base="xs:string">
                                                                <xs:maxLength
value="21"/>
                                                            </xs:restriction>
                                                        </xs:simpleType>
                                                    </xs:element>
                                                    <xs:element
name="Decodificacion_Unidad_Tramitacion_Inicio" minOccurs="0" maxOccurs="1">
                                                        <xs:simpleType>
                                                            <xs:restriction
base="xs:string">
                                                                <xs:maxLength
value="120"/>
                                                            </xs:restriction>
                                                        </xs:simpleType>
                                                    </xs:element>
                                                </xs:sequence>
                                            </xs:complexType>
                                        </xs:element>
                                        <xs:element                 name="De_Formulario_Generico"
minOccurs="0" maxOccurs="1">
                                         <xs:complexType>
                                            <xs:sequence>
                                             <xs:element       minOccurs="1"       maxOccurs="1"
name="Expone">
                                                <xs:simpleType>
                                                 <xs:restriction base="xs:string">
                                                    <xs:maxLength value="4000"/>
                                                 </xs:restriction>
                                                </xs:simpleType>
                                             </xs:element>
                                             <xs:element       minOccurs="1"       maxOccurs="1"
name="Solicita">
                                                <xs:simpleType>
                                                 <xs:restriction base="xs:string">
                                                    <xs:maxLength value="4000"/>
                                                 </xs:restriction>
                                                </xs:simpleType>
```

```
                                    </xs:element>
                                </xs:sequence>
                            </xs:complexType>
                        </xs:element>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:schema>
```

Representación gráfica del esquema del mensaje de control

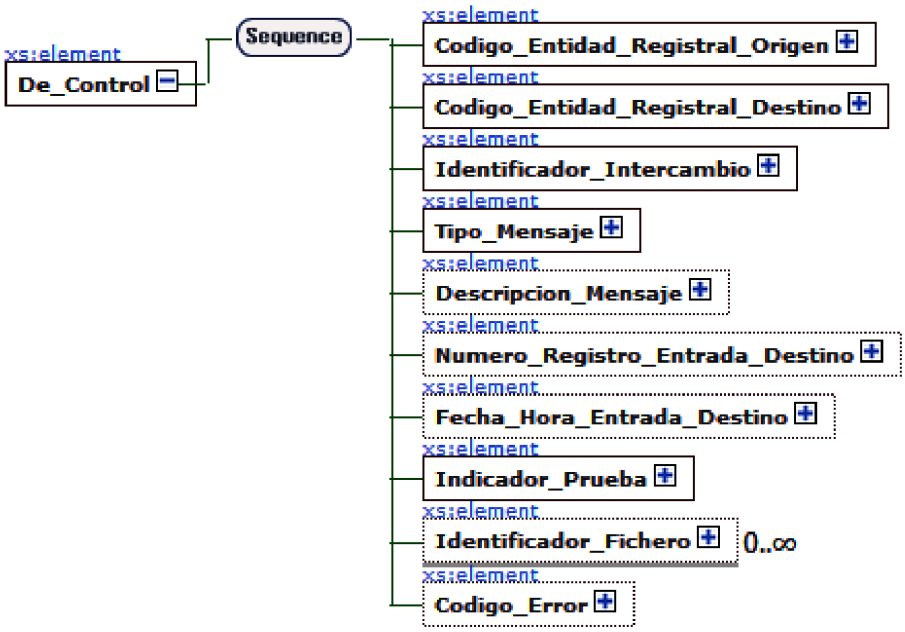



**Figura 18.** EsquemaXML: Mensaje de control – Visión general

Esquema XML del mensaje de control

```
<xs:schema elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="De_Control">
  <xs:complexType>
   <xs:sequence>
    <xs:element minOccurs="1" maxOccurs="1"
name="Codigo_Entidad_Registral_Origen">
     <xs:simpleType>
```

```
        <xs:restriction base="xs:string">
          <xs:maxLength value="21"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element                    minOccurs="1"                    maxOccurs="1"
name="Codigo_Entidad_Registral_Destino">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="21"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="1" maxOccurs="1" name="Identificador_Intercambio">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="33"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="1" maxOccurs="1" name="Tipo_Mensaje">
       <xs:simpleType>
        <xs:restriction base="xs:string">
                          <xs:maxLength value="2"/>
                          <xs:enumeration value="01"/>
                          <xs:enumeration value="02"/>
                          <xs:enumeration value="03"/>
                          <xs:enumeration value="04"/>
                          <xs:enumeration value="05"/>
                          <xs:enumeration value="06"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="0" maxOccurs="1" name="Descripcion_Mensaje">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="1024"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element                    minOccurs="0"                    maxOccurs="1"
name="Numero_Registro_Entrada_Destino">
       <xs:simpleType>
```

```
        <xs:restriction base="xs:string">
          <xs:maxLength value="20"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="0" maxOccurs="1"
name="Fecha_Hora_Entrada_Destino">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="19"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="1" maxOccurs="1" name="Indicador_Prueba">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="0"/>
          <xs:enumeration value="1"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="0" maxOccurs="unbounded"
name="Identificador_Fichero">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="50"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="0" maxOccurs="1" name="Codigo_Error">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="4"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
     </xs:sequence>
    </xs:complexType>
   </xs:element>
</xs:schema>
```

# § 24

## Resolución de 19 de febrero de 2013, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Reutilización de recursos de la información

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 54, de 4 de marzo de 2013
Última modificación: sin modificaciones
Referencia: BOE-A-2013-2380

La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público establece la regulación aplicable a la reutilización de la información elaborada o custodiada por las instancias públicas, en base a la potencialidad que le otorga el desarrollo de la sociedad de la información, el gran interés para las empresas a la hora de operar en sus ámbitos de actuación, contribuir al crecimiento económico y la creación de empleo, y para los ciudadanos como elemento de transparencia y guía para la participación democrática.

El Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal introduce en su disposición final primera dos modificaciones en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica; en primer lugar se añade un nuevo párrafo l) a la disposición adicional primera, apartado 1, del citado Real Decreto 4/2010 para añadir una Norma Técnica de Interoperabilidad sobre reutilización de recursos de información; y, en segundo lugar, se introduce una disposición adicional quinta sobre la norma técnica relativa a la reutilización de recursos de información por la cual se señala el plazo en que dicha norma deberá estar aprobada.

Las normas técnicas de interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas normas técnicas de interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de administración electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

En particular, la Norma técnica de interoperabilidad de reutilización de recursos de información establece condiciones comunes sobre selección, identificación, descripción, formato, condiciones de uso y puesta a disposición de los documentos y recursos de

información elaborados o custodiados por el sector público, relativos a numerosos ámbitos de interés como la información social, económica, jurídica, turística, sobre empresas, educación, etc., cumpliendo plenamente con lo establecido en la citada Ley 37/2007, de 16 de noviembre.

Estas condiciones tienen el objetivo de facilitar y garantizar el proceso de reutilización de la información de carácter público procedente de las Administraciones públicas, asegurando la persistencia de la información, el uso de formatos así como los términos y condiciones de uso adecuados.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma técnica de interoperabilidad de reutilización de recursos de información cuyo texto se incluye a continuación.

**Segundo.**

La Norma técnica de interoperabilidad de reutilización de recursos de información que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

## NORMA TÉCNICA DE INTEROPERABILIDAD DE REUTILIZACIÓN DE RECURSOS DE INFORMACIÓN

### *I. Objeto*

La Norma técnica de interoperabilidad de reutilización de recursos de información tiene por objeto establecer el conjunto de pautas básicas para la reutilización de documentos y recursos de información elaborados o custodiados por el sector público a los que se refiere el artículo 3 de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público por cualquier agente interesado.

### *II. Ámbito de aplicación*

Esta norma será de aplicación para la puesta a disposición, para su reutilización, de recursos de información de carácter público por parte de cualquier órgano de la Administración pública o Entidad de Derecho Público vinculada o dependiente de aquella en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

A los efectos de esta norma, las definiciones, palabras, expresiones y términos se entenderán en el sentido indicado en el glosario incluido en el anexo I.

### *III. Selección de la información reutilizable*

1. Al objeto de seleccionar los documentos y recursos de información aptos para la reutilización, se considerarán prioritarios los de mayor relevancia y potencial social y económico.

2. Los documentos y recursos de información reutilizables serán primarios, evitando las modificaciones o alteraciones de la información existente en la fuente, al objeto de evitar errores que se puedan producir durante la manipulación de la información.

3. El nivel granular será el más fino posible, evitando agregaciones adicionales, para posibilitar una reutilización adecuada a cualquier necesidad.

4. Los documentos y recursos de información reutilizables tendrán asociada información estructurada que permita su procesamiento automatizado.

5. Los documentos y recursos de información de elaboración o recogida periódica puestos a disposición para su reutilización estarán actualizados a sus últimas versiones y se indicará la fecha de última actualización, así como el periodo de la misma.

*IV. Identificación de la información reutilizable*

1. Los documentos y recursos de información reutilizables estarán identificados mediante referencias únicas y unívocas, basadas en identificadores de recursos uniformes, que componen la base necesaria para habilitar un mecanismo coherente de reutilización de la información a través de Internet. Con el uso de estos identificadores se podrá hacer referencia a los documentos o recursos que representan de forma unívoca, estable, extensible, persistente en el tiempo y ofreciendo garantías de procedencia, requisitos clave para facilitar su posterior reutilización.

2. Para la construcción de los identificadores de recursos uniformes se tendrán en cuenta los siguientes requisitos:

a) Se usarán los protocolos HTTP o HTTPS, con el fin de garantizar el direccionamiento y resolución de cualquier identificador de los recursos en la web.

b) Dado que pueden existir representaciones distintas asociadas a un mismo recurso de información, un servidor al que se le solicita un identificador de recurso uniforme debería gestionar dicha petición en función de la cabecera HTTP recibida, devolviendo la representación del recurso adecuada a las preferencias del cliente.

c) Para la composición de los identificadores de recursos uniformes se usará un esquema consistente, extensible y persistente, preferentemente de acuerdo con el esquema definido en el anexo II. Las normas de construcción de los mismos seguirán unos patrones determinados que ofrezcan coherencia en la uniformidad, los cuales podrán ser ampliados o adaptados en caso de necesidad. Aquellos Identificadores que sean creados y publicados en algún momento, deberán mantenerse en el tiempo.

d) Los identificadores de recursos uniformes seguirán una estructura de composición comprensible y significativa. El identificador deberá ofrecer información de manera que pueda ser entendido y fácilmente escrito por personas lo que permitirá disponer de información sobre el propio recurso, así como su procedencia únicamente interpretando el identificador.

e) El identificador de recursos uniforme que identifica cada documento o recurso, en la medida de lo posible, no revelará información sobre la implementación técnica de generación del recurso representado.

*V. Descripción de la información reutilizable*

1. Para la descripción de los documentos y recursos de información reutilizables puestos a disposición pública se asociarán los metadatos mínimos recogidos en el anexo III; para los valores de ciertos metadatos se tendrá en cuenta lo establecido en los anexos IV y V.

2. Cada distribución tendrá asociados, al menos, los metadatos recogidos en el anexo III.

3. Para facilitar la reutilización de vocabularios se utilizará el Centro de Interoperabilidad Semántica de la Administración previsto en el artículo 10, apartado 3 del Real Decreto 4/2010, dichos vocabularios se publicarán de acuerdo con las condiciones de formato establecidas en el apartado VI.

*VI. Formato de los documentos y recursos de información reutilizables*

1. Con el objeto de garantizar la independencia en la elección de alternativas tecnológicas por los ciudadanos y las Administraciones públicas y la adaptabilidad al progreso de la tecnología, los documentos y recursos de información reutilizables puestos a disposición pública, los metadatos y los servicios asociados a los mismos utilizarán estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean

de uso generalizado por la ciudadanía, siendo de aplicación lo previsto en el artículo 11 del Real Decreto 4/2010, de 8 de enero y se ceñirán a lo establecido en la Norma técnica de interoperabilidad de catálogo de estándares, aprobada por Resolución de 3 de octubre de 2012, de la Secretaría de Estado de Administraciones Públicas.

2. Se podrán utilizar otros estándares cuando existan particularidades que lo justifiquen, cuando no sea viable la conversión a un estándar más adecuado o, bien no exista alternativa, siendo de aplicación lo previsto sobre estándares en el artículo 11 del Real Decreto 4/2010, de 8 de enero.

3. Cualquier documento o recurso de información reutilizable podrá ser puesto a disposición pública a través de una o varias distribuciones en varios formatos distintos, con el objeto de facilitar la reutilización a agentes con distintos perfiles.

4. Se seleccionarán preferentemente formatos que ofrezcan representación semántica de la información, con el fin de facilitar una mejor comprensión de la información representada y su tratamiento automatizado. Si los formatos elegidos lo permiten, se priorizará el uso de esquemas o vocabularios internacionalmente reconocidos para representar la información.

5. Se incluirá preferentemente información de ayuda complementaria sobre los esquemas o vocabularios utilizados para representar la información.

*VII. Términos y condiciones de uso aplicables*

1. Las condiciones de reutilización específica de los órganos y entidades de Derecho Público de las Administraciones públicas se ajustarán a lo dispuesto en la Ley 37/2007, de 16 de noviembre, y su normativa de desarrollo. Lo establecido en el artículo 8 del Real Decreto 1495/2011, de 24 de octubre, podrá ser utilizado como referencia por otras Administraciones Públicas.

2. Dichas condiciones de reutilización globales a un organismo, disponibles en formato digital y procesables electrónicamente, podrán ser complementadas por condiciones específicas aplicadas a categorías de documentos o recursos de información concretos mediante licencias-tipo, disponibles en las mismas condiciones que las globales.

*VIII. Puesta a disposición de los documentos y recursos de información*

1. Los documentos o recursos de información puestos a disposición públicamente atenderán al principio de accesibilidad a la información y a los servicios por medios electrónicos en los términos establecidos por la normativa vigente, según lo establecido en el artículo 4.c) de la Ley 11/2007, de 22 de junio.

2. Cada órgano, organismo o entidad de derecho público del ámbito establecido en el artículo 1.2 del Real Decreto 1495/2011, de 11 de octubre, proporcionará información estructurada sobre los documentos y recursos de información susceptibles de reutilización, preferentemente a través de un espacio dedicado en su sede electrónica con el Localizador de Recurso Uniforme correspondiente, según el modelo http://www.sede.gob.es/datosabiertos. El resto de los órganos y entidades de derecho público de las Administraciones públicas seguirá sus normas reguladoras específicas.

3. Se asociará a los documentos o recursos de información reutilizables puestos a disposición pública la información necesaria que permita su interpretación.

4. En el caso de que se realice una puesta a disposición de la información mediante puntos de acceso dinámico, complementarios a los puntos de descarga masiva, se elaborará un documento técnico explicativo sobre el uso y configuración de estos puntos de acceso con, al menos, los parámetros de consulta permitidos, el tipo de información devuelta y los formatos aceptados.

5. Las direcciones electrónicas que alberguen documentos, recursos de información o catálogos de información pública susceptibles de reutilización contendrán información de aviso de dicha condición.

*IX. Catálogo de información pública reutilizable*

1. A efectos de la colaboración de los distintos órganos y entidades, los catálogos de información pública reutilizable implementarán:

a) Una interfaz de publicación, que permita a los diferentes órganos y entidades públicos poner a disposición los metadatos de sus documentos y recursos de información reutilizables.

b) Una interfaz de consulta, que permita que las aplicaciones de terceros puedan acceder a funcionalidades de búsqueda.

2. La descripción de cada categoría de documentos o recursos de información se realizará en fichas donde se recogerán, al menos, los metadatos obligatorios, descritos en el anexo III. Para la definición de catálogos y registros se podrá aplicar el modelo de plantilla incluido en el anexo VI.

3. Se proporcionará acceso al contenido del catálogo de dos formas:

a) Mediante documentos HTML legibles para las personas.

b) Mediante información procesable automáticamente que permita la reutilización de los propios metadatos del catálogo y la interoperabilidad con otros catálogos. El propio catálogo se ofrecerá como un conjunto de datos reutilizable, utilizando para ello el vocabulario internacionalmente reconocido DCAT.

## ANEXO I

## Glosario

Agente reutilizador: persona, física o jurídica que reutilice información del sector público, ya sea para fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública.

Dato: Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para comunicación, interpretación o procesamiento por medios automáticos o humanos.

Distribución: Información en un formato concreto, accesible desde un URL concreto. Un recurso de información puede disponer de una o múltiples distribuciones.

Documento: Toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos.

Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Documentos o recursos de información reutilizable: Documentos que obran en poder de las Administraciones, órganos y entidades de Derecho Público del sector público, por personas físicas o jurídicas, con fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública, de acuerdo con el ámbito de aplicación y exclusiones establecidos en el artículo 3 de la Ley 37/2007, de 16 de noviembre.

Documento o recurso de información primario: Dato tal y como se capta de la fuente sin modificaciones o alteraciones.

Extensiones multipropósito de correo de Internet (Multipurpose Internet Mail Extensions): Serie de convenciones o especificaciones dirigidas al intercambio, a través de Internet, de todo tipo de ficheros –texto, audio, vídeo, u otros– de forma transparente para el usuario.

Formato: Conjunto de características técnicas y de presentación de un recurso de información o documento.

Identificador de Recursos Uniforme: Cadena alfanumérica compacta que identifica recursos –físicos o abstractos– en la web de forma unívoca. La diferencia respecto a un Localizador de Recursos Uniforme es su invariabilidad en la referencia de recursos.

Infraestructura de Descripción de Recursos: Marco para la descripción semántica de recursos en la web, de manera que se dota de sentido a las representaciones en la web para que los datos puedan ser procesables automáticamente. RDF no es un formato, sino que existen distintas formas de representación –XML, N3, Turtle, etc.

Interfaz de Programación de Aplicaciones: Punto de comunicación entre componentes de software, que ofrece un conjunto de llamadas a librerías de programación que ofrecen acceso a servicios desde los procesos, consiguiendo la abstracción en la programación entre niveles inferiores y superiores del software.

Linked Open Data: Aproximación de ciertas iniciativas de apertura de datos (Open Data) basada en tecnologías de la Web Semántica, donde se relacionan datos definidos de forma semántica y que están identificados y representados en la web.

Localizador de Recursos Uniforme: Término usado para denominar ciertos identificadores de recursos uniformes cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo.

Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

Nivel de granularidad: Es el nivel de detalle de los datos, en la medida en la que trata el nivel más atómico por el cual se definen los datos.

Ontología: Descripción formal de los conceptos y relaciones que pueden existir sobre agentes o una comunidad. Especificación consensuada que describe un dominio de información.

Open Data: Iniciativa de apertura de datos aptos para su reutilización por parte de terceros.

Punto de acceso dinámico: Servicio de consulta que permite obtener información estructurada a través de peticiones basadas en parámetros configurables.

RDFa: Forma de representación de datos estructurados presentes en documentos web mediante anotaciones semánticas (RDF), incluidas en el código e invisibles para el usuario, que permiten a las aplicaciones interpretar esta información y utilizarla de forma eficaz.

SPARQL (SPARQL Protocol and RDF Query Language): Tecnología de consulta de información sobre diversas fuentes de datos que almacenan los mismos siguiendo el modelo de descripción RDF.

Tripleta RDF: Sentencia en la que se describe la relación de un recurso con otro a través de un sujeto, un predicado (o propiedad), y un objeto.

W3C (World Wide Web Consortium): Consorcio neutro internacional de reconocido prestigio donde las organizaciones Miembro, el personal a tiempo completo y el público en general, trabajan conjuntamente para desarrollar estándares para la web.

Web Semántica: infraestructura de tecnologías y mecanismos que ofrece la posibilidad de definir, integrar, compartir y reutilizar información en la web entre distintas partes de forma automatizada en función de su significado.

*Acrónimos y abreviaturas*

API: Application Programming Interface (Interfaz de Programación de Aplicaciones).

DCAT: Data Catalog Vocabulary (Vocabulario de Catálogo de Datos).

HTTP: Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto).

HTTPS: HTTP Secure (Protocolo de Transferencia de Hipertexto Seguro).

MIME: Multipurpose Internet Mail Extensions (Extensiones multipropósito de correo de Internet).

OWL: Web Ontology Language (Lenguaje de Ontologías Web).

RDF: Resource Description Framework (Infraestructura de Descripción de Recursos).

RDF-S: RDF Schema (Esquema para la Infraestructura de Descripción de Recursos).

RSS: RDF Site Summary (Resumen del Sitio en RDF) o Really Simple Syndication (Sindicación Realmente Simple).

SKOS: Simple Knowledge Organization System (Sistema de Organización del Conocimiento Simple).

URI: Uniform Resource Identifier (Identificador de Recurso Uniforme).

URL: Uniform Resource Locator (Localizador de Recurso Uniforme).

WWW: World Wide Web.

**ANEXO II**

**Esquema de URI**

El esquema de identificadores de recursos uniformes o URI establece un mecanismo de identificación común para los datos que se exponen públicamente, de forma que se pueda hacer referencia a estos de forma única, fiable y persistente en el tiempo, requisito clave para facilitar su posterior reutilización.

*Características básicas del esquema a implementar*

Los requisitos genéricos para diseñar el esquema de URI son los siguientes:

a) Utilizar el protocolo HTTP, de forma que se garantiza la resolución de cualquier URI en la web.

b) Usar una estructura de composición de URI consistente, extensible y persistente. Las normas de construcción de los URI seguirán unos patrones determinados que ofrezcan coherencia en la uniformidad, los cuales podrán ser ampliados o adaptados en caso de necesidad.

c) Los URI seguirán una estructura de composición comprensible y relevante. Esto significa que el propio identificador debe ofrecer información semántica autocontenida, lo que permitirá a cualquier agente reutilizador disponer de información sobre el propio recurso, así como su procedencia.

d) No se debe exponer información sobre la implementación técnica de los recursos que representan los URI. En la medida de lo posible se omitirá información específica sobre la tecnología subyacente del recurso representado; por ejemplo, no se incluirán las extensiones correspondientes a tecnologías con las que se generan los recursos web como.php,.jsp, etc.

e) Los URI deben cumplir el principio de persistencia, lo que significa que los que ya han sido creados previamente nunca deberían variar, y que el contenido al que hacen referencia, debería ser accesible. En el caso de que sea necesario cambiar o eliminar el recurso al que apunta un identificador, se deberá establecer un mecanismo de información sobre el estado del recurso usando los códigos de estado de HTTP. En el caso de poder ofrecer una redirección a la nueva ubicación del recurso, se utilizarán los códigos de estado HTTP 3XX, mientras que para indicar que un recurso ha desaparecido permanentemente se utilizará el código de estado HTTP 410.

*Estructura básica de los URI*

Todos los URI tendrán una estructura uniforme que ofrecerá coherencia al sistema de representación de los recursos, cubrirá los principios básicos de construcción de las mismas y contendrá información intuitiva sobre la procedencia y el tipo de información que identifica.

La base de los URI incluirá información básica sobre la procedencia de los datos, que representará un espacio dedicado por parte de la entidad para albergar su plataforma de reutilización; para indicar la situación de la información relativa a la iniciativa de datos abiertos –portal web, catálogo, u otra información sobre el proyecto– se utilizará preferentemente www.sede.gob.es/datosabiertos o bien http://organismo.gob.es/datosabiertos cuando los recursos no se ubiquen en una sede electrónica. El resto de los recursos semánticos podrán seguir un patrón dependiente únicamente del dominio (http://organismo.gob.es).

Para el caso de los URI de la documentación en los portales web de los organismos, cabe en su caso determinar primero el idioma, según la norma internacional correspondiente ISO 639-1, y después el canal, según el modelo http://organismo.gob.es/idioma/datosabiertos, por ejemplo http://organismo.gob.es/es-ES/datosabiertos. Esto dependerá de las políticas y de las características tecnológicas de cada organismo. Esto no será necesario en la gestión de recursos semánticos, ya que su propia descripción admite varios idiomas para el mismo recurso con un URI único.

Los elementos que componen la ruta de un URI son: sector, carácter de la información, tipo de representación, dominio o temática y los conceptos específicos. Dentro de la composición de una URI se especifican por el siguiente orden:

http://{base}/{carácter}[/{sector}][/{dominio}][/{concepto}][.{ext}]

O, alternativamente, utilizando los identificadores de fragmento mediante la marca «#» al final de la dirección:

http://{base}/{carácter}[/{sector}][/{dominio}][.{ext}][#{concepto}]

Esta estructura general de un URI puede variar dependiendo de las necesidades o preferencias de una organización, siendo obligatorio mantener invariables los elementos base y carácter. La parte final del URI, podría identificar la temática general o específica del recurso, el concepto concreto que representa y/o el formato de representación mediante una extensión. Estos dos últimos componentes son opcionales dependiendo del tipo de información que represente.

Carácter:

| Valor | Información que representa |
|---|---|
| Catálogo. | Documento o recurso de información incluido en el catálogo, con una lista de recursos o entidades de un mismo dominio. Habitualmente estos documentos y recursos de información contendrían datos comunes como condiciones de uso, origen, vocabularios utilizados, etc. También identifica al catálogo en sí. |
| Def. | Vocabulario u ontología utilizada como modelo semántico. Habitualmente esquemas RDF-S u ontologías representadas mediante OWL. |
| Kos. | Sistema de organización del conocimiento sobre un dominio concreto. Habitualmente taxonomías, diccionarios o tesauros, representados mediante SKOS. |
| Recurso. | Identificación abstracta única y unívoca de un recurso u objeto físico o conceptual. Estos recursos son las representaciones atómicas de los documentos y recursos de información y suelen ser instancias de los conceptos que se definen en los vocabularios. Si se especifica extensión (o formato) en el URI indica que es la representación del recurso.<br>Pueden existir dos tipos de representaciones de un recurso básicas: un documento legible para humanos –normalmente HTML– o para las máquinas, en cualquiera de los formatos de representación de RDF. El tipo concreto del documento será especificado mediante extensiones del propio documento. |

Sector:

La selección de un sector adecuado, acompañado del dominio específico del origen, le dará a cualquier usuario la confianza de conocer el tipo de información que está manejando y la fuente de la misma. Se seleccionará un identificador del sector (primario), según lo especificado en el anexo IV. Cada documento o recurso de información, vocabulario o esquema de conceptos debe pertenecer a un único sector. Si pertenece a más de uno, se utilizará el más representativo o alguno que se pueda considerar común.

Dominio o temática de la información:

Para identificar los elementos específicos dentro de un sector –recursos de información, vocabularios, esquemas de conceptos, etc.–, se creará una referencia adecuada que represente al dominio o temática de la información tratada.

Conceptos específicos:

Los últimos elementos de ciertos URI –tras el carácter, sector y nombre del dominio de la información– incluyen a los conceptos e instancias específicas de recursos. Los conceptos son representaciones abstractas que se corresponden con las clases o propiedades de los vocabularios u ontologías utilizados para representar semánticamente los recursos. Además del concepto, se podrá representar una referencia unívoca a instancias concretas. También se podrán representar esquemas de conceptos abstractos, dentro de sistemas de gestión del conocimiento (taxonomías, tesauros, etc.).

Formato:

Dado que los documentos que representan recursos pueden ser de diversos tipos, éstos se identificarán a través de la extensión del propio fichero, como, por ejemplo, «doc.html», «doc.rdf» o «doc.n3». Para la identificación de los recursos de forma abstracta se omitirá la extensión.

A continuación, se especifican los tipos de URI específicos para recursos semánticos de una iniciativa basada en Linked Data.

*URI para identificar catálogos y conjuntos de datos*

Si la iniciativa de reutilización sólo dispone de un catálogo, se podría representar a través del URI: http://{base}/catalogo

En el caso de que el organismo disponga de más de un catálogo se definirá una referencia descriptiva para cada catálogo que haga referencia al tema o dominio del mismo. Para ello se utilizará el URI: http://{base}/catalogo/{sector}

Los conjuntos de datos incluidos en cada catálogo se identifican mediante un URI con un identificador único para cada conjunto de datos: http://{base}/catalogo/{dataset}

O, en su defecto, utilizando la nomenclatura de identificadores de fragmentos (#): http://{base}/catalogo#{dataset}

*URI para identificar vocabularios*

Cualquier vocabulario u ontología seguirá el esquema: http://{base}/def/{sector}/{dominio}

Donde sector indicará el tema del vocabulario y dominio corresponderá a la referencia asignada al vocabulario, una representación textual breve pero descriptiva.

Las clases y propiedades del vocabulario tendrán como base el URI correspondiente al vocabulario donde se definen, compuesto con los identificadores de las clases o propiedades según el esquema: http://{base}/def/{sector}/{dominio}/{propiedad|Clase}

O, en su defecto, utilizando la nomenclatura de identificadores de fragmentos (#): http://{base}/def/{sector}/{dominio}#{propiedad|Clase}

*URI para identificar esquemas de conceptos*

Cualquier sistema de organización del conocimiento –taxonomías, diccionarios, tesauros, etc.– sobre un dominio concreto será identificado mediante un esquema de URI basado en la estructura: http://{base}/kos/{sector}/{dominio}

Donde sector indicará el tema del esquema de conceptos y dominio corresponderá a la referencia asignada a dicho esquema de clasificación. Ésta referencia del dominio será una breve representación textual pero descriptiva.

Los conceptos incluidos en el esquema tendrán como base el URI correspondiente al esquema donde se definen y tendrán la forma: http://{base}/kos/{sector}/{dominio}/{Concepto}

O, en su defecto, utilizando la nomenclatura de identificadores de fragmentos (#): http://{base}/kos/{sector}/{dominio}#{Concepto}

*URI para identificar a cualquier instancia física o conceptual*

Estos recursos son las representaciones atómicas de los documentos y recursos de información. A su vez suelen ser instancias de las clases que se definen en los vocabularios. Estos recursos se identifican mediante el esquema: http://{base}/recurso/{sector}[/{dominio}]/{clase}/{ID}

O, en su defecto, utilizando la nomenclatura de identificadores de fragmentos (#): http://{base}/recurso/{sector}[/{dominio}]/{clase}#{ID}

Donde sector indicará el tema relacionado con el recurso y clase corresponderá al tipo de concepto que describe al recurso. Habitualmente coincide con el identificador de una de las clases que caracteriza al recurso. El ID es un identificador que permite distinguir al recurso entre el resto de las instancias del mismo tipo, dentro del sistema. El dominio, relativo al recurso, podría corresponder al especificado en el propio vocabulario que define las clases de la instancia, es opcional.

*Normalización de los componentes de los URI*

Para garantizar la coherencia y el mantenimiento posterior del esquema de URI se aplicarán las siguientes reglas para normalizar las distintas partes que componen los URI:

a) Seleccionar identificadores alfanuméricos cortos únicos, que sean representativos, intuitivos y semánticos.

b) Usar siempre minúsculas, salvo en los casos en los que se utilice el nombre de la clase o concepto. Habitualmente, los nombres de las clases se representan con el primer carácter de cada palabra en mayúsculas.

c) Eliminar todos los acentos, diéresis y símbolos de puntuación. Como excepción puede usarse el guión (–).

d) Eliminar conjunciones y artículos en los casos de que el concepto a representar contenga más de una palabra.

e) Puede usarse el guión (–) como separador entre palabras.

f) Evitar en la medida de lo posible la abreviatura de palabras, salvo que la abreviatura sea intuitiva.

Los términos que componen los URI deberán ser legibles e interpretables por el mayor número de personas posible, por lo que se utilizará el castellano o cualquiera de las lenguas oficiales.

*Prácticas relativas a la gestión de recursos semánticos a través de URI*

Se aplicarán las prácticas siguientes para la gestión de recursos semánticos descritos en RDF:

a) Siempre que sea posible, y existan versiones del recurso en formato legible para personas HTML o similar y RDF, el servidor que gestiona los URI realizará negociación del contenido en función de la cabecera del agente que realiza la petición. En el caso de que el cliente acepte un formato de representación RDF en cualquiera de sus notaciones (p.e., especificando en su cabecera que acepta el tipo MIME application/rdf+xml) se servirá el documento RDF a través del mecanismo de redirecciones alternativas mediante los códigos de estado HTTP 3XX. De la misma forma, si es posible, se servirá la representación en cualquier otro formato preferido por el cliente.

b) En el caso de que no se realice una negociación del contenido desde el servidor y, para favorecer el descubrimiento de contenido RDF desde los documentos HTML relacionados con las descripciones de los recursos, se incluirán enlaces a la representación alternativa en cualquiera de las representaciones en RDF desde los propios documentos HTML de la forma <link rel=«alternate» type=«application/rdf+xml» href=«documento.rdf»> o similar. En esa sentencia se incluye el tipo de formato MIME del documento (application/rdf +xml, text/n3, etc.).

c) Cuando se establezcan enlaces entre distintos recursos de información, se procurará la generación de enlaces que conecten los recursos bidireccionales para facilitar la navegación sobre los recursos de información en ambos sentidos.

## ANEXO III

### Metadatos de documentos y recursos de información del catálogo

A continuación se describen los distintos metadatos asociados con el catálogo y los documentos y recursos de información incluidos en él, además del término recomendado para su representación usando vocabularios estándar que se identifican por las abreviaturas de su espacio de nombres. Además de la denominación, descripción del metadato y el tipo de dato que se deberá usar para la representación, se especifica si es obligatorio –columna R (requerido)– y si admite más de un metadato de ese tipo –columna M (múltiple), como podría ser en el caso de las descripciones en distintos idiomas.

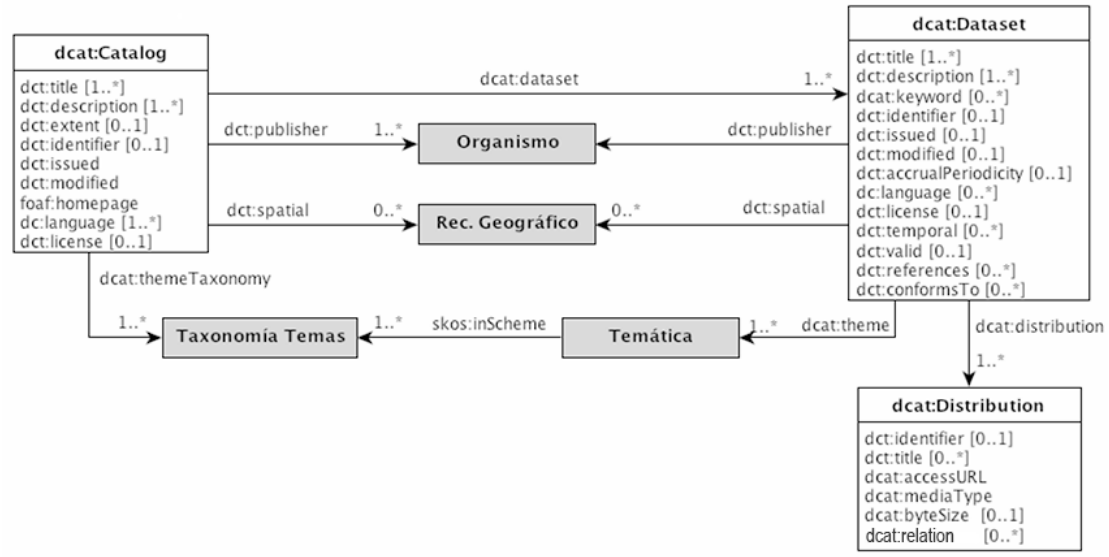
Para la descripción y exposición de los metadatos recogidos en este anexo se usarán los vocabularios y esquemas de valores propuestos, mediante tecnologías de la Web Semántica –al menos, la descripción de recursos en RDF en cualquiera de sus formatos de representación–, al objeto de facilitar la interoperabilidad a nivel semántico de los sistemas que compartan esta representación estándar.

Vocabularios:

| Vocabulario | URI |
|---|---|
| XML Schema | xsd: http://www.w3.org/2001/XMLSchema# |
| Simple Knowledge Organization System (SKOS) | skos: http://www.w3.org/2004/02/skos/core# |
| Dataset Catalog (dcat) | dcat: http://www.w3.org/ns/dcat# |
| Dublin Core Terms | dct: http://purl.org/dc/terms/ |
| Dublin Core Elements | dc: http://purl.org/dc/elements/1.1/ |
| W3C Time Ontology | time: http://www.w3.org/2006/time# |
| Friend Of A Friend (FOAF) | foaf: http://xmlns.com/foaf/0.1/ |

La representación semántica se basa en el vocabulario DCAT, desarrollado por la entidad World Wide Web Consortium (W3C) y que permite la estandarización en la definición de catálogos de documentos y recursos de información. Un catálogo de documentos y recursos de información se representa mediante instancias de tipo dcat:Catalog e incluye una colección de (dcat:Dataset). Estas instancias tienen propiedades que hacen referencia a otros recursos y conceptos semánticos identificados en los anexos del presente documento y que son representados gráficamente en el siguiente diagrama y detalladas a continuación. Las entidades o propiedades básicas que se detallan en este anexo podrán ser enriquecidas con metadatos adicionales que se estimen oportunos para la mejora de la calidad de la información.

Al menos, los recursos que representen al catálogo de datos y a sus conjuntos de datos deberán ser identificado mediante un URI específico que siga el esquema de definido en el anexo II.




| Catálogo (dominio dcat: Catalog) | | | | | |
|---|---|---|---|---|---|
| **Metadato** | **Descripción** | **propiedad** | **R** | **M** | **Tipo y Esquema de valores** |
| Nombre | Breve título o nombre dado al catálogo de datos. | dct:title | ✓ | ✓ | Literal. Cadena alfanumérica (se recomienda en varios idiomas). |
| Descripción | Resumen descriptivo del catálogo de datos. | dct:description | ✓ | ✓ | Literal. Cadena alfanumérica (se recomienda en varios idiomas). |
| Órgano publicador | Entidad que publica el catálogo. | dct:publisher | ✓ | – | foaf:Agent. Se especificará el URI correspondiente a un órgano público diferenciados por un código alfanumérico único para cada órgano/unidad/oficina, que será extraído del Directorio Común gestionado por el MINHAP según el esquema siguiente: http://datos.gob.es/recurso/sector- publico/org/ Organismol(ID- MINHAP} |
| Tamaño del catálogo | Número total de documentos y recursos de información inventariados en el catálogo. | dct:extent | – | – | dct:SizeOrDuration. Se recomienda incluir el valor de un número entero y su representación textual equivalente. |
| Identificador | Referencia para identificar el catálogo. | dct:identifier | – | – | xsd:anyURI. URI que identifica la descripción actual del catálogo. |
| Fecha de creación | Fecha de publicación inicial del catálogo | dct:issued | ✓ | – | Literal. Fecha/Hora con formato ISO-8601: YYYY-MM-DDThh:mm:ssTZD. |
| Fecha de actualización | Fecha en la que se modificó por última vez el catálogo (se añade, elimina o modifica un documento o recurso de información). | dct:modified | ✓ | – | Literal. Fecha/Hora con formato ISO-8601: YYYY-MM-DDThh:mm:ssTZD. |
| Idioma(s) | Idioma(s) en el(los) que se proporciona la información del catálogo. | dc:language | ✓ | ✓ | Literal. Valores normalizados de etiquetas para identificar idiomas definidos en el RFC 5646 («es», «ga», «ca», «eu», «en», «fr»}. Se usará una etiqueta por cada propiedad. |

| Catálogo (dominio dcat: Catalog) | | | | | |
|---|---|---|---|---|---|
| **Metadato** | **Descripción** | **propiedad** | **R** | **M** | **Tipo y Esquema de valores** |
| Cobertura geográfica | Ámbito geográfico cubierto por el catálogo. | dct:spatial | – | ✓ | Recurso. Se aplicará preferentemente lo establecido al respecto en el anexo V. Un recurso por propiedad. |
| Temáticas | Totalidad de materias incluidas en el catálogo. | dcat:themeTaxo-nomy | ✓ | ✓ | skos:ConceptScheme. Se aplicará preferentemente la taxonomía definida en el anexo IV. Su valor es: http://datos.gob.es/kos/sector-publico/sector/ |
| Página web | Dirección web de acceso al catálogo de datos (acceso para el público). | foaf:homepage | ✓ | – | Recurso. URI que referencia a la portada del catálogo. |
| Términos de uso | Referencia a los términos de uso generales del catálogo. | dct:license | ✓ | – | Recurso. URI que referencia al recurso que describe los términos de uso. |
| Documento(s) y recurso(s) de información | Lista de cada uno de los documentos y recursos de información del catálogo. | dcat:dataset | ✓ | ✓ | dcat:Dataset. Tendrá tantas propiedades como entradas en el catálogo. (Ver metadatos de documentos y recursos de información). |

| Documento y recurso de información (dominio dcat: Dataset) | | | | | |
|---|---|---|---|---|---|
| **Metadato** | **Descripción** | **propiedad** | **R** | **M** | **Tipo y Esquema de valores** |
| Nombre | Nombre o título del documento o recurso de información. | dct: title | ✓ | ✓ | Literal. Cadena alfanumérica (se recomienda en varios idiomas). |
| Descripción | Descripción detallada del documento o recurso de información. | dct :description | ✓ | ✓ | Literal. Cadena alfanumérica (se recomienda en varios idiomas). |
| Temática(s) | Temática o materia primaria del documento o recurso de información. | dcat: theme | ✓ | ✓ | skos:Concept. Se recomienda hacer referencia a un tema asociado con el sector público, según la taxonomía definida en el anexo IV. |
| Etiqueta(s) | Etiqueta(s) textual(es) que permiten categorizar libremente el documento o recurso de información. | dcat:keyword | – | ✓ | Literal. Cadena alfanumérica compacta. Pueden incluirse varias propiedades (una por etiqueta). |
| Identificador | URI que identifica al documento o recurso de información. | det:identifie | – | – | xsd:anyURI. URI que identifica la ficha descriptiva del documento o recurso de información. |
| Fecha de creación | Fecha de creación del documento o recurso de información. | dct : issued | – | – | Literal. Fecha/Hora con formato ISO-8601: YYYY-MM-DDThh:mm:ssTZD. |
| Fecha de última actualización | Última fecha conocida en la que se modificó o actualizó el contenido del documento o recurso de información. | det:modified | – | – | Literal. Fecha/Hora con formato ISO-8601: YYYY-MM-DDThh:mm:ssTZD. |
| Frecuencia de actualización | Periodo de tiempo aproximado transcurrido entre actualizaciones del documento o recurso de información, si hubiera | dct : accrualPeriodicity | – | – | dct:Frequency. Se recomienda especificar periodos normalizados con formato ISO-8601 (PT), o similar. |
| Idioma(s) | Idioma(s) en el(los) que se encuentra la información del documento o recurso de información. | dc:language | – | ✓ | Literal. Valores normalizados de etiquetas para identificar idiomas definidos en el RFC 5646 («es», «ga», «ca», «eu», «en», «fr»}. Se usará una etiqueta por propiedad. |
| Organismo que expone y publica los datos | Organismo que publica el documento o recurso de información. | dct:publisher | ✓ | – | foaf:Agent. Se especificará el URI correspondiente a un organismo público diferenciados por un código alfanumérico único para cada órgano/ unidad/oficina, que será extraído del Directorio Común gestionado por el MINHAP según el esquema siguiente: http:lldatos.gob.es/recu rso/sector-publico/org/Organismo){ID-MINHAP } |
| Condiciones de uso | Recurso que describe las condiciones de uso o licencia específica aplicable al propio documento o recurso de información. | dct : license | – | – | dct:LicenseDocument o similar. Se especificará un URI que referencia al recurso que define las condiciones de uso. Si no es una licencia-tipo, y si fuese necesario, en la descripción se podría indicar contraprestación económica utilizando valores del código de divisa normalizado por el estándar ISO-4217 (EUR, USD, GBP, etc.). |
| Cobertura geográfica | Ámbito geográfico cubierto por el documento o recurso de información. | dct:spatial | – | ✓ | Recurso. Puede tomar uno de los valores que representan las provincias españolas, según se expresan en el anexo V. |
| Cobertura temporal | Fecha de inicio, fin y la duración del periodo cubierto por el documento o recurso de información. | dct: temporal | – | ✓ | dct:PeriodOfTime. Periodo de tiempo que puede ser definido mediante la ontología de Tiempo del W3C (time:) |
| Vigencia del recurso | Fecha de validez de un documento o recurso de información o en la que se estima una modificación o actualización de su contenido. | dct:valid | – | – | Literal. Fecha/Hora con formato ISO-8601: YYYY-MM-DDThh:mm:ssTZD. |
| Recurso(s) relacionado(s) | Enlaces a recursos relacionados con el documento o recurso de información (información sobre los propios datos, material audiovisual, etc.). | dct : references | – | ✓ | Recurso. URI que identifica al recurso relacionado. Se pueden incluir tantas propiedades como referencias se conozcan. |
| Normativa | Normativa relativa al documento o recurso de información. Es un enlace a un documento legal. | dct : conformsTo | – | ✓ | Recurso. URI que identifica al documento legal relacionado. Se pueden incluir tantas propiedades como documentos normativos se conozcan. |
| Distribución(es) | Referencia a los recursos que identifican los volcados del documento o recurso de información en sus posibles formatos. | dcat:distribution | ✓ | ✓ | dcat:Distribution. URI que identifica al recurso que describe una distribución del documento o recurso de información. Puede tener tantas propiedades como distribuciones se conozcan. |

| Distribución de documento o recurso de información (dominio dcat: Distribution) | | | | | |
|---|---|---|---|---|---|
| **Metadato** | **Descripción** | **propiedad** | **R** | **M** | **Tipo y Esquema de valores** |
| Identificador | URI que identifica a la distribución. | la dct:identifie | – | – | xsd:anyURI. URI que identifica la ficha descriptiva de la distribución. |
| Nombre | Breve título o nombre dado a la distribución. | dct:title | – | ✓ | Literal. Cadena alfanumérica (se recomienda en varios idiomas). |
| URL de acceso | URL que permite el acceso al volcado o consulta de los documentos o recursos de información. | dcat : accessURL | ✓ | – | Literal. URL con la dirección del documento, o servicio que permite la obtención de los datos. |
| Formato | Formato en que se encuentra representado el documento o recurso de información. | dcat:mediaType | ✓ | – | dct:MediaTypeOrExtent. Recurso que indica el tipo MIME del formato de los datos. Únicamente se especificará un formato por distribución. |
| Tamaño | Tamaño aproximado del documento o recurso de información. | dcat:byteSize | – | – | Literal. El tamaño será descrito en bytes. |
| Información adicional sobre formato | Enlace(s) relacionado(s) con el formato, el donde se indica el formato, el esquema utilizado para su representación u otra información técnica sobre cómo acceder a los documentos o recursos de información. | dct:relation | – | ✓ | Recurso. URI con una referencia a un recurso asociado con el formato. Se pueden incluir tantas propiedades como referencias a documentos adicionales se conozcan. |

## ANEXO IV

### Metadatos de documentos y recursos de información del catálogo

Taxonomía de sectores primarios donde se especifican los temas relacionados a cada uno de ellos. Esta clasificación ha sido elaborada con base en el documento «Propuesta de Taxonomía Común para los procedimientos y servicios electrónicos, el marco de la Ley 11/2007», y comparando su propuesta de materias con las temáticas empleadas en otros portales de referencia como 060, EUGO, INE, EUROSTAT, WORLD BANK, OECD.

Esta clasificación servirá de base común para componer el esquema de URI expresado en el anexo II y para la categorización de los catálogos de recursos de información pública y sus registros, según los metadatos especificados en el anexo III.

| Sector | Identificador |
|---|---|
| Ciencia y tecnología:<br>Incluye: Innovación, Investigación, I+D+i, Telecomunicaciones, Internet y Sociedad de la Información. | ciencia-tecnologia |
| Comercio:<br>Incluye: Consumo. | comercio |
| Cultura y ocio:<br>Incluye: Tiempo libre. | cultura-ocio |
| Demografía:<br>Incluye: Inmigración y Emigración, Familia, Mujeres, Infancia, Mayores, Padrón. | demografia |
| Deporte:<br>Incluye: Instalaciones deportivas, Federaciones, Competiciones. | deporte |
| Economía:<br>Incluye: Deuda, Moneda y Banca y finanzas. | economia |
| Educación:<br>Incluye: Formación. | educacion |
| Empleo:<br>Incluye: Trabajo, Mercado laboral. | empleo |
| Energía:<br>Incluye: Fuentes renovables | energia |
| Hacienda:<br>Incluye: Impuestos. | hacienda |
| Industria:<br>Incluye: Minería. | industria |
| Legislación y justicia:<br>Incluye: Registros. | legislacion-justicia |
| Medio ambiente:<br>Incluye: Meteorología, Geografía, Conservación fauna y flora. | medio-ambiente |
| Medio Rural:<br>Incluye: Agricultura, Ganadería, Pesca y Silvicultura. | medio-rural-pesca |
| Salud:<br>Incluye: Sanidad. | salud |
| Sector público:<br>Incluye: Presupuestos, Organigrama institucional, Legislación interna, Función pública. | sector-publico |
| Seguridad:<br>Incluye: Protección civil, Defensa. | seguridad |
| Sociedad y bienestar:<br>Incluye: Participación ciudadana, Marginación, Envejecimiento Activo, Autonomía personal y Dependencia, Invalidez, Jubilación, Seguros y Pensiones, Prestaciones y Subvenciones. | sociedad-bienestar |
| Transporte:<br>Incluye: Comunicaciones y Tráfico. | transporte |
| Turismo:<br>Incluye: Alojamientos, Hostelería, Gastronomía. | turismo |
| Urbanismo e infraestructuras:<br>Incluye: Saneamiento público, Construcción (infraestructuras, equipamientos públicos). | urbanismo-infraestructuras |
| Vivienda:<br>Incluye: Mercado inmobiliario, Construcción (viviendas). | vivienda |

En la tabla siguiente se identifican los sectores primarios detallados anteriormente y se especifican los URI que se usarán como referencia unívoca de cada concepto. Dichos identificadores son los valores que tomarán los metadatos que categorizan por temática a los

recursos de información y que se definen en el anexo III. Esta taxonomía está definida como un esquema de conceptos identificado mediante el URI:

http://datos.gob.es/kos/sector-publico/sector

El URI de cada uno de los conceptos se compondrá concatenando la palabra que lo identifica, expresado en la tabla anterior, a la base del URI del esquema de conceptos.

| Sector | URI |
|---|---|
| Ciencia y tecnología | http://datos.gob.es/kos/sector-publico/sector/ciencia-tecnologia |
| Comercio | http://datos.gob.es/kos/sector-publico/sector/comercio |
| Cultura y ocio | http://datos.gob.es/kos/sector-publico/sector/cultura-ocio |
| Demografía | http://datos.gob.es/kos/sector-publico/sector/demografia |
| Deporte | http://datos.gob.es/kos/sector-publico/sector/deporte |
| Economía | http://datos.gob.es/kos/sector-publico/sector/economia |
| Educación | http://datos.gob.es/kos/sector-publico/sector/educacion |
| Empleo | http://datos.gob.es/kos/sector-publico/sector/empleo |
| Energía | http://datos.gob.es/kos/sector-publico/sector/energia |
| Hacienda | http://datos.gob.es/kos/sector-publico/sector/hacienda |
| Industria | http://datos.gob.es/kos/sector-publico/sector/industria |
| Legislación y justicia | http://datos.gob.es/kos/sector-publico/sector/legislacion-justicia |
| Medio ambiente | http://datos.gob.es/kos/sector-publico/sector/medio-ambiente |
| Medio Rural | http://datos.gob.es/kos/sector-publico/sector/medio-rural-pesca |
| Salud | http://datos.gob.es/kos/sector-publico/sector/salud |
| Sector público | http://datos.gob.es/kos/sector-publico/sector/sector-publico |
| Seguridad | http://datos.gob.es/kos/sector-publico/sector/seguridad |
| Sociedad y bienestar | http://datos.gob.es/kos/sector-publico/sector/sociedad-bienestar |
| Transporte | http://datos.gob.es/kos/sector-publico/sector/transporte |
| Turismo | http://datos.gob.es/kos/sector-publico/sector/turismo |
| Urbanismo e infraestructuras. | http://datos.gob.es/kos/sector-publico/sector/urbanismo-infraestructuras |
| Vivienda | http://datos.gob.es/kos/sector-publico/sector/vivienda |

## ANEXO V

### Metadatos de documentos y recursos de información del catálogo

Identificadores correspondientes a los recursos geográficos del territorio español –País, Autonomías y Provincias– que se utilizarán como referencia de estos elementos de forma unívoca en el proceso de descripción de los metadatos de cobertura geográfica correspondientes a los catálogos de recursos de información, según lo especificado en el anexo III; los identificadores expresados en la segunda columna de las tablas son los valores que puede tomar el metadato.

| País | URI |
|---|---|
| España | http://datos.gob.es/recurso/sector-publico/territorio/Pais/España |

| Comunidad/Ciudad Autónoma | URI |
|---|---|
| Andalucía | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Andalucia |
| Aragón | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Aragon |
| Principado de Asturias | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Principado-Asturias |
| Illes Balears | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Illes-Balears |
| Canarias | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Canarias |
| Cantabria | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Cantabria |
| Castilla y León | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Castilla-Leon |
| Castilla-La Mancha | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Castilla-La-Mancha |
| Cataluña | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Cataluna |
| Comunitat Valenciana | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Comunitat-Valenciana |
| Extremadura | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Extremadura |
| Galicia | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Galicia |
| Comunidad de Madrid | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Comunidad-Madrid |
| Región de Murcia | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Region-Murcia |
| C. Foral de Navarra | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Comunidad-Foral-Navarra |
| País Vasco | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Pais-Vasco |
| La Rioja | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/La-Rioja |
| Ceuta | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Ceuta |
| Melilla | http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Melilla |

| Comunidad/Ciudad Autónoma | Provincia | URI Identificador |
|---|---|---|
| Andalucía | Almería | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Almeria |
| | Cádiz | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Cadiz |
| | Córdoba | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Cordoba |
| | Granada | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Granada |
| | Huelva | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Huelva |
| | Jaén | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Jaen |
| | Málaga | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Malaga |
| | Sevilla | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Sevilla |
| Aragón | Huesca | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Huesca |
| | Teruel | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Teruel |
| | Zaragoza | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Zaragoza |
| Principado de Asturias | Asturias | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Asturias |
| Illes Balears | Illes Balears | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Illes-Balears |
| Canarias | Las Palmas | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Las-Palmas |
| | Santa Cruz de Tenerife | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Santa-Cruz-Tenerife |
| Cantabria | Cantabria | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Cantabria |
| Castilla y León | Ávila | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Avila |
| | Burgos | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Burgos |
| | León | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Leon |
| | Palencia | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Palencia |
| | Salamanca | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Salamanca |
| | Segovia | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Segovia |
| | Soria | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Soria |
| | Valladolid | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Valladolid |
| | Zamora | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Zamora |
| Castilla-La Mancha | Albacete | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Albacete |
| | Ciudad Real | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Ciudad-Real |
| | Cuenca | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Cuenca |
| | Guadalajara | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Guadalajara |
| | Toledo | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Toledo |
| Cataluña | Barcelona | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Barcelona |
| | Girona | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Girona |
| | Lleida | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Lleida |
| | Tarragona | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Tarragona |
| Comunitat Valenciana | Alicante/Alacant | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Alicante |
| | Castellón/Castelló | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Castellon |
| | Valencia/València | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Valencia |
| Extremadura | Badajoz | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Badajoz |
| | Cáceres | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Caceres |
| Galicia | A Coruña | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/A-Coruna |
| | Lugo | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Lugo |
| | Ourense | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Ourense |
| | Pontevedra | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Pontevedra |
| Comunidad de Madrid | Madrid | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Madrid |
| Región de Murcia | Murcia | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Murcia |
| C. Foral de Navarra | Navarra | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Navarra |
| País Vasco | Álava | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Alava |
| | Guipúzcoa | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Guipuzcoa |
| | Vizcaya | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Vizcaya |
| La Rioja | La Rioja | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/La-Rioja |
| Ceuta | Ceuta | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Ceuta |
| Melilla | Melilla | http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Melilla |

## ANEXO VI

### Modelo de plantilla RDF de definición de catálogos y registros

Modelo de plantilla para la descripción en RDF de un catálogo de datos, registros, conjuntos de datos y distribuciones asociadas. La plantilla de documento se especifica en Notación 3 (N3) y también en RDF/XML. En ambas plantillas se incluyen partes variables, así como comentarios sobre los posibles valores a utilizar. En caso de que exista alguna propiedad que no tenga aplicación o no se conozca el valor, se preferirá no definir las propiedades a dejar elementos sin valor.

### Formato RDF/XML

```
<?xml version="1.0"?>
<rdf:RDF
  xmlns:time="http://www.w3.org/2006/time#"
  xmlns:dct="http://purl.org/dc/terms/"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:dcat="http://www.w3.org/ns/dcat#"
  xmlns:foaf="http://xmlns.com/foaf/0.1/"
```

```
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
  xmlns:tema="http://datos.gob.es/kos/sector-publico/sector/"
  xmlns:auto="http://datos.gob.es/recurso/sector-publico/
territorio/Autonomia/"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">

  <dcat:Catalog rdf:about="@@URI-catalogo@@">
    <!--
      Identificador que se corresponde con el URI que
identifica a el própio catálogo
      p.e., http://datos.gob.es/catalogo/catalogoNacional
    -->
    <dct:identifier>@@URI-catalogo@@</dct:identifier>
    <!--
      El título y la descripción se puede repetir varias
veces para ofrecer representaciones en idiomas distintos
    -->
    <dct:title xml:lang="es">@@título-es@@</dct:title>
    <dct:description xml:lang="es">@@descripción@@</
dct:description>
    <!--
      Organismo que publica el catálogo, se usará un URI que
lo describe:
      p.e., http://datos.gob.es/recurso/sector-publico/org/
Organismo/E00003901
    -->
    <dct:publisher rdf:resource="@@URI-organismo@@" />
    <!--
      Tamaño del catálogo (número de datasets) expresado
mediante un entero y
      texto(s) (soporta varios idiomas).
    -->
    <dct:extent>
      <dct:SizeOrDuration>
        <rdf:value
          rdf:datatype="http://www.w3.org/2001/
XMLSchema#nonNegativeInteger">@@número-entero@@</rdf:value>
        <rdfs:label xml:lang="es">@@número-texto@@</
rdfs:label>
      </dct:SizeOrDuration>
    </dct:extent>
    <!-- Las fechas tienen el formato YYYY-MM-DDTHH:MM:SS+TZ
-->
    <dct:issued rdf:datatype="http://www.w3.org/2001/
XMLSchema#dateTime">@@fecha-creación@@</dct:issued>
    <dct:modified rdf:datatype="http://www.w3.org/2001/
XMLSchema#dateTime">@@actualización@@</dct:modified>
    <!-- Idioma del catálogo (repetir la propiedad tantas
veces como idiomas) es|ga|en|ca|...-->
    <dc:language>@@código-idioma@@</dc:language>
    <!--
      La cobertura espacial del catálogo.
      Repetir la propiedad si es necesario haciendo
referencia a un recurso del estilo:
        - http://datos.gob.es/recurso/sector-publico/
territorio/pais/Espana
        - http://datos.gob.es/recurso/sector-publico/
territorio/autonomia/Extremadura
        - http://datos.gob.es/recurso/sector-publico/
territorio/provincia/Caceres
    -->
    <dct:spatial rdf:resource="@@URI-localización@@" />
    <!--
      Taxonomía de conceptos de temáticas:
        - http://datos.gob.es/kos/sector-publico/sector/
    -->
    <dcat:themeTaxonomy rdf:resource="http://datos.gob.es/kos/
sector-publico/sector/" />
```

```
    <!-- Página principal del própio catálogo, donde se
representa visualmente -->
    <foaf:homepage rdf:resource="@@URI-homepage-catálogo@@" />
    <!-- Enlace a recurso con los términos de uso generales
(recomendable con metadatos autocontenidos) -->
    <dct:license rdf:resource="@@URI-terminos-uso@@" />
    <!--
      Especificación de cada uno de los registros contenidos
en el catálogo.
      Repetir propiedad por cada documento o recurso de
información.
    -->
    <dcat:dataset>
      <dcat:Dataset rdf:about="@@URI-dataset@@">
        <!-- Identificador que se corresponde con el URI que
identifica a el propio dataset -->
        <dct:identifier>@@URI-dataset@@</dct:identifier>
        <!-- El título y la descripción del dataset -->
        <dct:title xml:lang="es">@@título-es@@</dct:title>
        <dct:description xml:lang="es">@@descripción@@</
dct:description>
        <!--
          Temática(s) primaria(s) del catálogo. Repetir la
propiedad si hay más de una.
          Usar el esquema de conceptos normalizado:
            - http://datos.gob.es/kos/sector-publico/sector/
ciencia-tecnologia
              http://datos.gob.es/kos/sector-publico/sector/
cultura-ocio
              http://datos.gob.es/kos/sector-publico/sector/
demografia
              http://datos.gob.es/kos/sector-publico/sector/
deporte
              http://datos.gob.es/kos/sector-publico/sector/
economia
              http://datos.gob.es/kos/sector-publico/sector/
educacion
              http://datos.gob.es/kos/sector-
publico/sector/empleo
              http://datos.gob.es/kos/sector-publico/sector/
energia
              http://datos.gob.es/kos/sector-publico/sector/
hacienda
              http://datos.gob.es/kos/sector-publico/sector/
industria
              http://datos.gob.es/kos/sector-publico/sector/
legislacion-justicia
              http://datos.gob.es/kos/sector-
publico/sector/medio-ambiente
              http://datos.gob.es/kos/sector-
publico/sector/medio-rural
              http://datos.gob.es/kos/sector-
publico/sector/salud
              http://datos.gob.es/kos/sector-publico/sector/
sector-publico
              http://datos.gob.es/kos/sector-publico/sector/
seguridad
              http://datos.gob.es/kos/sector-publico/sector/
sociedad-bienestar
              http://datos.gob.es/kos/sector-publico/sector/
transporte
              http://datos.gob.es/kos/sector-publico/sector/
turismo
              http://datos.gob.es/kos/sector-publico/sector/
urbanismo-infraestructuras
              http://datos.gob.es/kos/sector-publico/sector/
vivienda
        -->
        <dcat:theme rdf:resource="@@URI-sector-temático@@" />
```

```
        <!-- Palabra(s) clave, que indica(n) conceptos
temáticos alternativos al tema primario -->
        <dcat:keyword>@@palabra-clave@@</dcat:keyword>
        <!-- Las fechas pueden ser de tipo
            - http://www.w3.org/2001/XMLSchema#date (YYYY-MM-
DD)
            - http://www.w3.org/2001/XMLSchema#dateTime (YYYY-
MM-DDTHH:MM:SS+TZ)
        -->
        <dct:issued rdf:datatype="http://www.w3.org/2001/
XMLSchema#date">@@creación@@</dct:issued>
        <dct:modified rdf:datatype="http://www.w3.org/2001/
XMLSchema#date">@@actualiz.@@</dct:modified>
        <!--
          Periodo de actualización estimada de los datos del
dataset.
          -->
          <dct:accrualPeriodicity>
          <dct:Frequency>
            <rdfs:label>Cada @@intervalo-tiempo@@</rdfs:label>
            <rdf:value>
              <time:DurationDescription>
               <rdfs:label>@@intervalo-tiempo@@</rdfs:label>
               <!-- puede ser time:days o otra magnitud
(weeks, months, etc.) -->
               <time:days rdf:datatype="http://
www.w3.org/2001/XMLSchema#decimal">@@n@@</time:days>
              </time:DurationDescription>
            </rdf:value>
          </dct:Frequency>
        </dct:accrualPeriodicity>
        <!-- Idioma(s) en los que están especificados los
datos (@@es|en|ca|ga...) -->
        <dc:language>@@idioma@@</dc:language>
        <!-- Organismo que expone los datos. Se usará un URI
que lo identifique. -->
        <dct:publisher rdf:resource="@@URI-organismo@@" />
        <!-- URI donde se describe las condiciones de uso
aplicables a los datos -->
        <dct:license rdf:resource="@@URI-licencia@@" />
        <!--
          La cobertura espacial de los datos
          Repetir la propiedad si es necesario, haciendo
referencia a un recurso del estilo:
            - http://datos.gob.es/recurso/sector-publico/
territorio/Pais/Espana
            - http://datos.gob.es/recurso/sector-publico/
territorio/Autonomia/Extremadura
            - http://datos.gob.es/recurso/sector-publico/
territorio/Provincia/Caceres
        -->
        <dct:spatial rdf:resource="@@URI-localización@@" />
        <!--
          La cobertura temporal de los datos (En el caso que
sea necesario)
          Se define el inicio y el fin mediante xsd:dateTime
(YYYY-MM-DDTHH:MM:SS+TZ)
        -->
        <dct:temporal>
          <time:Interval>
            <rdf:type rdf:resource="http://purl.org/dc/terms/
PeriodOfTime" />
            <time:hasBeginning>
              <time:Instant>
                <time:inXSDDateTime rdf:datatype="http://
www.w3.org/2001/XMLSchema#dateTime">
                    @@fecha-hora-inicio@@
                </time:inXSDDateTime>
              </time:Instant>
```

```
            </time:hasBeginning>
            <time:hasEnd>
              <time:Instant>
                 <time:inXSDDateTime rdf:datatype="http://
www.w3.org/2001/XMLSchema#dateTime">
                   @@fecha-hora-fin@@
                 </time:inXSDDateTime>
              </time:Instant>
            </time:hasEnd>
          </time:Interval>
        </dct:temporal>
        <!-- Enlaces a recursos relacionados -->
        <dct:references rdf:resource="@@URI-recurso-
relacionado@@" />
        <!--
          Las distintas distribuciones (1..n)
        -->
        <dcat:distribution>
          <dcat:Distribution>
            <!-- Identificador que se corresponde con el URI
que identifica a la propia distribución -->
            <dct:identifier>@@URI-distribución@@</
dct:identifier>
            <dct:title xml:lang="es">@@nombre-distribucion-
es@@</dct:title>
            <!-- URL de acceso a los datos -->
            <dcat:accessURL
              rdf:datatype="http://www.w3.org/2001/
XMLSchema#anyURI">@@URL-acceso@@</dcat:accessURL>
            <!-- Formato MIME de los datos de la
distribución. -->
            <dct:format>
              <dct:IMT>
                <rdf:value>${valor_MIME_Type (p.e.,
text/csv)}</rdf:value>
                <rdfs:label>${texto_legible_ (p.e., CSV)}</
rdfs:label>
              </dct:IMT>
            </dct:format>
            <!--
              Tamaño de la distribución del documento o
recurso de información.
              Se representa en bytes (número decimal) y con
una etiqueta textual legible (p.e., 30KB)
            -->
            <dcat:byteSize rdf:datatype="http://
www.w3.org/2001/XMLSchema#decimal">
                  @@num-bytes@@
            </dcat:byteSize>
            <!--
              Si se conoce algún documento con información
adicional sobre los datos y el
              acceso a los mismos, se puede hacer referencia
mediante un texto y la URL al documento
            -->
            <dct:relation>
              <rdf:Description>
                <rdfs:label xml:lang="es">@@texto-enlace@@</
rdfs:label>
                <foaf:page rdf:resource="@@URL-documento@@" />
              </rdf:Description>
            </dct:relation>
          </dcat:Distribution>
        </dcat:distribution>
      </dcat:Dataset>
    </dcat:dataset>
  </dcat:Catalog>
</rdf:RDF>
```

**Notación 3 (N3)**

```
@prefix dct: <http://purl.org/dc/terms/>.
@prefix dc: <http://purl.org/dc/elements/1.1/>.
@prefix dcat: <http://www.w3.org/ns/dcat#>.
@prefix foaf: <http://xmlns.com/foaf/0.1/>.
@prefix xsd: <http://www.w3.org/2001/XMLSchema#>.
@prefix tema: <http://datos.gob.es/kos/sector-
publico/sector/>.
@prefix time: <http://www.w3.org/2006/time#>.
@prefix xml: <http://www.w3.org/XML/1998/namespace>.
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#>.
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>.
@prefix auto: <http://datos.gob.es/recurso/sector-publico/
territorio/Autonomia/>.


#El catálogo
$$URI-catalogo$$ a dcat:Catalog;
   dct:title "$$título-es$$"@es;
   dct:description "$$descripción$$"@es;
   dct:identifier "$$URI-catalogo";
   # Número de conjuntos de datos
   dct:extent
   [
      a dct:SizeOrDuration;
      rdf:value "$$número-entero$$"^^xsd:nonNegativeInteger;
      rdfs:label "$$número-texto$$"@es.
   ];
   # Fechas de creación y actualización
   dct:issued "$$fecha-creación$$"^^xsd:dateTime;
   dct:modified "$$actualización$$"^^xsd:dateTime;
   dc:language "$$código-idioma$$";
   dct:publisher <$$URI-organismo$$>;
   dct:license <$$URI-términos-uso$$>;
   dct:spatial <$$URI-localización$$>;
   dcat:themeTaxonomy <http://datos.gob.es/kos/sector-
publico/sector/>;
   foaf:homepage <$$URI-homepage-catálogo$$>;

   # Conjuntos de datos que pertenecen al catálogo
(múltiples)
   dcat:dataset <$$URI-dataset$$>.


# Los conjuntos de datos asociados al catálogo
<$$URI-dataset$$> a dcat:Dataset;
   dct:title "$$título-es$$"@es;
   dct:description "$$descripción$$"@es;
   dcat:theme <$$URI-sector-temático$$>;
   dcat:keyword "$$palabra-clave$$","$$palabra-clave2$$","$
$palabra-claveN$$";
   # Frecuencia de actualización aproximada
   dct:accrualPeriodicity
   [
      a dct:Frequency;
      rdf:value
      [
         a time:DurationDescription;
         rdfs:label "$$intervalo-tiempo$$";
         time:days $$n$$.
      ];
      rdfs:label "Cada $$intervalo-tiempo$$".
   ];
   dct:publisher <$$URI-organismo$$>;
   dct:identifier "$$URI-dataset$$";
   dct:issued "$$creació$$"^^xsd:date;
   dct:modified "$$actualización$$"^^xsd:date;
```

```
   dc:language "$$idioma$$";
   dct:license <$$URI-licencia$$>;
   dct:spatial <$$URI-localización$$>;
   dct:references <$$URI-dataset$$>;
   dct:temporal
   [
      a dct:PeriodOfTime, time:Interval;
      time:hasBeginning
      [
         a time:Instant;
         time:inXSDDateTime "$$fecha-hora-inicio$
$"^^xsd:dateTime.
      ];
      time:hasEnd
      [
         a time:Instant;
         time:inXSDDateTime "$$fecha-hora-fin$
$"^^xsd:dateTime.
      ].
   ];
   # Cada una de las distribuciones del documento o recurso
de información
   dcat:distribution
   [
      a dcat:Distribution;
      dct:identifier "$$URI-distribución$$";
      dct:title "$$nombre-distribucion-es$$"@es;
      dct:format
      [
         a dct:IMT;
         rdf:value "${valor_MIME_Type (p.e., text/csv)}";
         rdfs:label "${texto_legible_ (p.e., CSV)}".
      ];
      dct:relation
      [
         rdfs:label "$$texto-enlace$$"@es;
         foaf:page <$$URL-documento$$>.
      ];
      dcat:accessURL "$$URL-acceso$$"^^xsd:anyURI;
      dcat:byteSize "$$num-bytes-texto$$".   ].
```

# § 25

## Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 106, de 4 de mayo de 2022
Última modificación: sin modificaciones
Referencia: BOE-A-2022-7191

I

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) tenía por objeto determinar la política de seguridad en la utilización de medios electrónicos de las entidades de su ámbito de aplicación, estando constituido por los principios básicos y requisitos mínimos que han venido garantizando adecuadamente la seguridad de la información tratada y los servicios prestados por dichas entidades.

El ENS, cuyo ámbito de aplicación comprendía todas las entidades de las administraciones públicas, perseguía fundamentar la confianza en que los sistemas de información prestan sus servicios adecuadamente y custodian la información sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a personas no autorizadas, estableciendo medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de forma que se facilite a los ciudadanos y a las administraciones públicas el ejercicio de sus derechos y el cumplimiento de sus obligaciones a través de medios electrónicos.

Desde 2010 se han producido notables cambios en España y en la Unión Europea, incluidos la progresiva transformación digital de nuestra sociedad, el nuevo escenario de la ciberseguridad y el avance de las tecnologías de aplicación. Asimismo, se ha evidenciado que los sistemas de información están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, advirtiéndose un notable incremento de los ciberataques, tanto en volumen y frecuencia como en sofisticación, con agentes y actores con mayores capacidades técnicas y operativas; amenazas que se producen en un contexto de alta dependencia de las tecnologías de la información y de las comunicaciones en nuestra sociedad y de gran interconexión de los sistemas de información. Todo ello afecta significativamente a un número cada vez mayor de entidades públicas y privadas, a sus cadenas de suministro, a los ciudadanos y, por ende, a la ciberseguridad nacional, lo que compromete el normal desenvolvimiento social y económico del país y el ejercicio de los derechos y libertades de los ciudadanos, como reconocen tanto la Estrategia de Ciberseguridad Nacional de 2013 como, particularmente, la Estrategia Nacional de Ciberseguridad 2019.

El Real Decreto 3/2010, de 8 de enero, establecía que el ENS debía desarrollarse y perfeccionarse manteniéndose actualizado de forma permanente conforme al progreso de los servicios de la administración electrónica, de la evolución de la tecnología, de los nuevos

estándares internacionales sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo.

En el plano normativo, acompasado a dichos cambios y en ocasiones como origen de los mismos, desde 2010 se han modificado tanto el marco europeo (con cuatro Reglamentos y una Directiva) como el español, referido a la seguridad nacional, regulación del procedimiento administrativo y el régimen jurídico del sector público, de protección de datos personales y de la seguridad de las redes y sistemas de información, y se ha evolucionado el marco estratégico de la ciberseguridad.

Así, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, considera a la ciberseguridad como un ámbito de especial interés de la Seguridad Nacional tal como señala su artículo 10, y que, por ello, requiere una atención específica por resultar básica para preservar los derechos y libertades y el bienestar de los ciudadanos y para garantizar el suministro de los servicios y recursos esenciales. De acuerdo con las previsiones de su artículo 4.3 se aprobó el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017, y posteriormente, el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, identificando en ambas al ciberespacio como un espacio común global, que la Estrategia 2021 describe como espacio de conexión caracterizado por su apertura funcional, la carencia de fronteras físicas y su fácil accesibilidad, añadiendo que en los espacios comunes globales resulta difícil la atribución de cualquier acción irregular o delictiva, dada su extensión, su débil regulación y la ausencia de soberanía.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha ampliado el ámbito de aplicación del ENS a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos en su artículo 156.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13 incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

En desarrollo de las dos leyes anteriores, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, concreta en diferentes preceptos la obligación del cumplimiento de las medidas de seguridad previstas en el ENS, como los referidos al intercambio electrónico de datos en entornos cerrados de comunicación, los sistemas de clave concertada y otros sistemas de identificación de las personas interesadas, el archivo electrónico único o los portales de internet, entre otros.

Coincidente en el tiempo con la aprobación de las tres leyes mencionadas, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, actualizó el ENS a la luz de la experiencia y conocimiento en su aplicación, de la situación de la ciberseguridad del momento, y de la evolución del marco legal, para adecuarse a lo previsto en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (conocido como «Reglamento eIDAS»).

Con relación a las medidas de seguridad del ENS en el tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ordenó en su disposición adicional primera que dichas medidas de seguridad se implanten en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679, del

Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). De otra parte, la disposición adicional primera también prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales. Por último, y en el mismo sentido, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ha establecido en su artículo 37 la obligación de aplicar las medidas del ENS a los tratamientos de datos personales por parte de las autoridades públicas competentes.

Por otra parte, con relación a la seguridad de redes y sistemas de información, desde la entrada en vigor del Real Decreto 3/2010, de 8 de enero, se han aprobado en la Unión Europea dos Reglamentos y una Directiva que han fijado el marco de actuación en los ordenamientos nacionales.

Así, en primer lugar, el Reglamento (UE) N.º 526/2013 del Parlamento Europeo y del Consejo de 21 de mayo de 2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) N.º 460/2004. En segundo lugar, el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»).

En tercer lugar, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como «Directiva NIS (*Security of Network and Information Systems)*», que ha sido objeto de transposición en España por medio del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, señalando la necesidad de tener en cuenta el ENS en el momento de elaborar las disposiciones reglamentarias, instrucciones y guías, y adoptar las medidas aplicables a entidades del ámbito de aplicación de este. Este Real Decreto-ley 12/2018, de 7 de septiembre, ha sido desarrollado por el Real Decreto 43/2021, de 26 de enero, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad. Así, el Real Decreto 43/2021, de 26 de enero, establece que las medidas para el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero.

Tal como estableció la Estrategia de Seguridad Nacional de 2017, España precisa garantizar un uso seguro y responsable de las redes y sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable. En este sentido, el Consejo de Seguridad Nacional aprobó el 12 de abril de 2019 la Estrategia Nacional de Ciberseguridad 2019, publicada por Orden PCI/487/2019, de 26 de abril, con el propósito de fijar las directrices generales en el ámbito de la ciberseguridad de manera que se alcanzasen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017.

La Estrategia Nacional de Ciberseguridad 2019, contiene un objetivo general y cinco objetivos específicos, y, para alcanzarlos, se proponen siete líneas de acción con un total de 65 medidas. El primero de estos objetivos es la seguridad y resiliencia de las redes y sistemas de información y comunicaciones del sector público y de los servicios esenciales y se desarrolla a través de dos líneas de acción y veinticuatro medidas específicas entre las que figura la de asegurar la plena implantación del Esquema Nacional de Seguridad. Para desarrollar esta Estrategia, el Consejo de Ministros ha aprobado el 29 de marzo de 2022 el

Plan Nacional de Ciberseguridad, que prevé cerca de 150 iniciativas, entre actuaciones y proyectos, para los próximos tres años.

Asimismo, la Estrategia Nacional de Ciberseguridad 2019 señala entre sus objetivos la consolidación de un marco nacional coherente e integrado que garantice la protección de la información y de los datos personales tratados por los sistemas y redes del sector público y de los servicios, sean o no esenciales, recogiendo que su cumplimiento requiere la implantación de medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, mediante el desarrollo de nuevas soluciones, y el refuerzo de la coordinación y la adaptación del ordenamiento jurídico.

II

La evolución de las amenazas, los nuevos vectores de ataque, el desarrollo de modernos mecanismos de respuesta y la necesidad de mantener la conformidad y el alineamiento con las regulaciones europeas y nacionales de aplicación, exigen adaptar las medidas de seguridad a esta nueva realidad. Fortalecer la ciberseguridad demanda recursos económicos, humanos y tecnológicos que se han de dimensionar atendiendo al principio de proporcionalidad y al nivel de seguridad requerido, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa.

Por ello, en un mundo hiperconectado como el actual, implementar la seguridad en el ciberespacio se ha convertido en una prioridad estratégica. Sin embargo, el riesgo en el ciberespacio es demasiado grande para que el sector público o las empresas lo aborden por sí solos, pues ambos comparten el interés y la responsabilidad de enfrentar juntos ese reto. A medida que aumenta el papel de la tecnología en la sociedad, la ciberseguridad se convierte en un desafío cada vez mayor.

De hecho, el pasado 9 de marzo, el Parlamento Europeo ha aprobado por amplísima mayoría una Resolución sobre injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación. Tal como señala dicha Resolución en sus considerandos, las injerencias extranjeras constituyen un patrón de conducta que amenaza o afecta negativamente a valores, procedimientos democráticos, procesos políticos, la seguridad de Estados y ciudadanos y la capacidad de hacer frente a situaciones excepcionales. Las tácticas de injerencia extranjera, que se combinan a menudo para tener un mayor efecto, adoptan, entre otras formas, los ciberataques, la asunción del control de infraestructuras críticas, la desinformación, supresión de información, manipulación de plataformas de redes sociales y de sus algoritmos, operaciones de pirateo y filtración, amenazas y acoso para acceder a información sobre los votantes e interferir en la legitimidad del proceso electoral, personalidades e identidades falsas, ejercicio de presiones sobre ciudadanos extranjeros que viven en la Unión, instrumentalización de migrantes y espionaje.

Al tiempo que el escenario descrito ha venido consolidándose, se ha ido extendiendo la implantación del ENS, resultando de ello una mayor experiencia acumulada sobre su aplicación, a la vez que un mejor conocimiento de la situación gracias a las sucesivas ediciones del Informe Nacional del Estado de la Seguridad (INES), del cuerpo de guías de seguridad CCN-STIC y de los servicios y herramientas proporcionados por la capacidad de respuesta a incidentes de seguridad de la información, el CCN-CERT, del Centro Criptológico Nacional (CCN).

En definitiva, por todas las razones anteriormente expuestas es necesario actualizar el ENS para cumplir tres grandes objetivos.

En primer lugar, alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital. Se trata de reflejar con claridad el ámbito de aplicación del ENS en beneficio de la ciberseguridad y de los derechos de los ciudadanos, así como de actualizar las referencias al marco legal vigente y de revisar la formulación de ciertas cuestiones a la luz de éste, conforme a la Estrategia Nacional de Ciberseguridad 2019 y el Plan Nacional de Ciberseguridad, de forma que se logre simplificar, precisar o armonizar los mandatos del ENS, eliminar aspectos que puedan considerarse excesivos, o añadir aquellos otros que se identifican como necesarios.

En segundo lugar, introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. Ello aconseja la inclusión en el ENS del concepto de «perfil de cumplimiento específico» que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

En tercer lugar, facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

Por último, la aprobación de este real decreto se incardina también en la ejecución del Plan de Digitalización de las Administraciones Públicas 2021-2025, uno de los instrumentos principales para el cumplimiento del Plan de Recuperación, Transformación y Resiliencia y su Componente 11 denominado «Modernización de las Administraciones Públicas», así como para el desarrollo de las inversiones y reformas previstas en la agenda España Digital 2025. Dicho Plan de Digitalización contempla expresamente, entre sus reformas, la actualización del ENS con el fin de hacer evolucionar la política de seguridad de todas las entidades del sector público español, tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información. Dicha reforma se ve complementada con la constitución del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos que servirá de referencia para las demás administraciones públicas y contribuirá a mejorar el cumplimiento del ENS de las entidades en su alcance de servicio. Esta previsión ha sido respaldada por el Acuerdo de Consejo de Ministros de 25 de mayo de 2021 sobre actuaciones urgentes en materia de ciberseguridad que mandata la tramitación y aprobación de un real decreto que sustituya al Real Decreto 3/2010, de 8 de enero, como medida de refuerzo del marco normativo.

III

El real decreto se estructura en cuarenta y un artículos distribuidos en siete capítulos, tres disposiciones adicionales, una disposición transitoria, una disposición derogatoria, tres disposiciones finales y cuatro anexos.

El capítulo I comprende las disposiciones generales que regulan el objeto de la norma, su ámbito de aplicación, la referencia a los sistemas de información que traten datos personales y las definiciones aplicables. El ámbito de aplicación es el previsto en el artículo 2 de la Ley 40/2015, de 1 de octubre, al que se añaden los sistemas que tratan información clasificada, sin perjuicio de la normativa que resulte de aplicación, pudiendo resultar necesario complementar las medidas de seguridad de este real decreto con otras específicas para tales sistemas, derivadas de los compromisos internacionales contraídos por España o su pertenencia a organismos o foros internacionales en la materia. Asimismo los requisitos del ENS serán de aplicación a los sistemas de información de las entidades del sector privado, cuando de acuerdo con la normativa aplicable y en virtud de una relación contractual presten servicios a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas. Como se ha señalado anteriormente, considerando que la transformación digital ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan los servicios públicos y que el sector privado se encuentra igualmente inmerso en la transformación digital de sus procesos de negocio, ambos tipos de sistemas de información se encuentran expuestos al mismo tipo de amenazas y riesgos. Por ello, los operadores del sector privado que prestan servicios a las entidades del sector público, por razón de la alta imbricación de unos y otras, han de garantizar el mismo nivel de seguridad que se aplica a los sistemas y a la información en el ámbito del sector público, todo ello de conformidad, además, con los especiales requerimientos establecidos tanto en la Ley Orgánica 3/2018, de 5 de diciembre, como en la Ley Orgánica 7/2021, de 26 de mayo. Por otra parte, cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo

establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

El capítulo II, que comprende los artículos 5 a 11, regula los principios básicos que deben regir el ENS y que enumera en su artículo 5: seguridad integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua y reevaluación periódica; y diferenciación de responsabilidades.

El capítulo III se refiere a la Política de Seguridad y los requisitos mínimos para permitir una protección adecuada de la información y los servicios. En los artículos 12 a 27 se definen tales requisitos: organización e implantación del proceso de seguridad; gestión de riesgos, consistente en un proceso de identificación, análisis, evaluación y tratamiento de los mismos; gestión de personal; profesionalidad; autorización y control de los accesos; protección de las instalaciones; adquisición de productos de seguridad y contratación de servicios de seguridad; mínimo privilegio; integridad y actualización del sistema; protección de la información almacenada y en tránsito; prevención ante otros sistemas de información interconectados; registro de la actividad y detección de código dañino; incidentes de seguridad; continuidad de la actividad; y mejora continua del proceso de seguridad. Seguidamente, el artículo 28 indica que para el cumplimiento de tales requisitos mínimos deberán adoptarse las medidas recogidas en el anexo II, conforme a una serie de consideraciones al efecto. No obstante, tales medidas de seguridad podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que la protección que aportan es, al menos, equivalente, y satisfacen los principios básicos y requisitos mínimos indicados previamente. En el artículo 29 se hace un llamamiento a la utilización de infraestructuras y servicios comunes de las administraciones públicas en aras de lograr una mayor eficiencia y retroalimentación de las sinergias de cada colectivo. Por último, el artículo 30 establece la posibilidad de implementar perfiles de cumplimiento específicos, así como esquemas de acreditación de entidades de implementación de configuraciones seguras.

El capítulo IV versa sobre la auditoría de la seguridad, el informe del estado de la seguridad y la respuesta a incidentes de seguridad. La auditoría de la seguridad se desarrolla íntegramente en el artículo 31, detallando las características del procedimiento de auditoría, así como de los correspondientes informes. Por su parte, el artículo 32, relativo al informe del estado de la seguridad, destaca el papel de la Comisión Sectorial de Administración Electrónica en este ámbito, así como del CCN y los órganos colegiados competentes en el ámbito de la administración digital en la Administración General del Estado.

La prevención, detección y respuesta a incidentes de seguridad se regula en los artículos 33 y 34, separando, por un lado, los aspectos relativos a la capacidad de respuesta y, por otro, los relativo a la prestación de los servicios de respuesta a incidentes de seguridad, tanto a las entidades del Sector Público como a las organizaciones del sector privado que les presten servicios.

En el capítulo V, artículos 35 a 38, se definen las normas de conformidad, que se concretan en cuatro: Administración Digital, ciclo de vida de servicios y sistemas, mecanismos de control y procedimientos de determinación de la conformidad con el ENS.

Por su parte, el capítulo VI, compuesto por su único artículo, el 39, establece la obligación de actualización permanente, de acuerdo con el marco jurídico vigente en cada momento, la evolución de la tecnología y los estándares en materia de seguridad y sistemas, así como de las ya mencionadas nuevas amenazas y vectores de ataque.

Concluye el articulado de la parte dispositiva con el capítulo VII, que desarrolla el procedimiento de categorización de los sistemas de información, definiendo en el artículo 40 las categorías de seguridad y en el artículo 41 las facultades al respecto.

En cuanto a las tres disposiciones adicionales, la primera regula los programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público que desarrollarán el CCN y el Instituto Nacional de Administración Pública.

La segunda disposición adicional regula las instrucciones técnicas de seguridad, de obligado cumplimiento y las guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC).

Por último, la tercera disposición adicional establece el cumplimiento del llamado principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH, por sus siglas en inglés, *Do No Significant Harm)* y las condiciones del etiquetado climático y digital.

La disposición transitoria única fija un plazo de veinticuatro meses para que los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, alcancen su plena adecuación al ENS.

La disposición derogatoria suprime el Real Decreto 3/2010, de 8 de enero, así como cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Por último, la norma cuenta con tres disposiciones finales. La primera de ellas enumera los títulos competenciales; la segunda disposición final habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la su aplicación y desarrollo, sin perjuicio de las competencias de las comunidades autónomas para el desarrollo y ejecución de la legislación básica del Estado, y la disposición final tercera ordena la entrada en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

El real decreto se complementa con cuatro anexos: el anexo I regula las categorías de seguridad de los sistemas de información, detallando la secuencia de actuaciones para determinar la categoría de seguridad de un sistema; el anexo II detalla las medidas de seguridad; el anexo III se ocupa del objeto, niveles e interpretación de la Auditoría de la seguridad y, por último, el anexo IV incluye el glosario de términos y definiciones.

Con relación, en particular, al anexo II, este detalla las medidas de seguridad estructuradas en tres grupos: el marco organizativo, constituido por el conjunto de medidas relacionadas con la organización global de la seguridad; el marco operacional, formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin; y las medidas de protección, que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas. Como se ha dicho, la modificación del marco táctico y operativo en el que se desenvuelven las ciberamenazas y sus correlativas salvaguardas ha obligado a actualizar el elenco de medidas de seguridad del anexo II, con objeto de añadir, eliminar o modificar controles y sub-controles, al tiempo que se incluye un nuevo sistema de referencias más moderno y adecuado, sobre la base de la existencia de un requisito general y de unos posibles refuerzos, alineados con el nivel de seguridad perseguido. Todo ello se efectúa con el objetivo de afianzar de manera proporcionada la seguridad de los sistemas de información concernidos, y facilitar su implantación y auditoría.

IV

El real decreto, cuya aprobación está incluida en el Plan Anual Normativo de la Administración General del Estado para el año 2022, se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia).

Así, la norma es acorde con los principios de necesidad y eficacia en tanto que persigue un interés general al concretar la regulación del ENS desarrollando en este aspecto la Ley 40/2015, de 1 de octubre y otros aspectos concretos de la normativa nacional y de la Unión Europea mencionada en este preámbulo. La norma es también acorde con el principio de proporcionalidad, al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento, estableciéndose un marco normativo estable, integrado y claro. Durante el procedimiento de elaboración de la norma y aún en el contexto de la aplicación de las previsiones del artículo 27 de la Ley 50/1997, de 27 de noviembre, del Gobierno, por tratarse de una tramitación de urgencia acordada por el Consejo de Ministros, se han formalizado los trámites de audiencia e información pública, conforme a lo previsto en el artículo 133 de la Ley 39/2015, de 1 de octubre, y el artículo 26 de la Ley 50/1997, de 27 de noviembre, en cumplimiento del principio de transparencia,

quedando además justificados en el preámbulo los objetivos que persigue este real decreto. El proyecto se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y ha sido informado por la Comisión Nacional de los Mercados y la Competencia A.A.I. y la Agencia Española de Protección de Datos A.A.I.

Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación en materia de cargas administrativas, respecto de la normativa que desarrolla.

El real decreto se aprueba en ejercicio de las competencias previstas en los artículos 149.1.18.ª, 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, sobre las telecomunicaciones y sobre la seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital, con la aprobación previa de la Ministra de Hacienda y Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 3 de mayo de 2022,

DISPONGO:

CAPÍTULO I

**Disposiciones generales**

**Artículo 1.** *Objeto.*

1. Este real decreto tiene por objeto regular el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

3. Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

**Artículo 2.** *Ámbito de aplicación.*

1. El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.

2. Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales.

3. Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

La política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto

contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

4. Cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

**Artículo 3.** *Sistemas de información que traten datos personales.*

1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.

**Artículo 4.** *Definiciones.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el Glosario de términos incluido en el anexo IV.

## CAPÍTULO II

## Principios básicos

**Artículo 5.** *Principios básicos del Esquema Nacional de Seguridad.*

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en los riesgos.
c) Prevención, detección, respuesta y conservación.
d) Existencia de líneas de defensa.
e) Vigilancia continua.
f) Reevaluación periódica.
g) Diferenciación de responsabilidades.

**Artículo 6.** *La seguridad como un proceso integral.*

1. La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

**Artículo 7.** *Gestión de la seguridad basada en los riesgos.*

1. El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

2. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

**Artículo 8.** *Prevención, detección, respuesta y conservación.*

1. La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

2. Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

3. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

4. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

5. Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

**Artículo 9.** *Existencia de líneas de defensa.*

1. El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.

b) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

**Artículo 10.** *Vigilancia continua y reevaluación periódica.*

1. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

2. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

3. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

**Artículo 11.** *Diferenciación de responsabilidades.*

1. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.
2. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.
3. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

## CAPÍTULO III

## Política de seguridad y requisitos mínimos de seguridad

**Artículo 12.** *Política de seguridad y requisitos mínimos de seguridad.*

1. La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

a) Los objetivos o misión de la organización.
b) El marco regulatorio en el que se desarrollarán las actividades.
c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.
d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.
e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
f) Los riesgos que se derivan del tratamiento de los datos personales.

2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente.
No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización.
3. En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento. Los organismos públicos y entidades pertenecientes al sector público institucional estatal podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del Departamento con el que mantenga la relación de vinculación, dependencia o adscripción, o bien quedar comprendidos en el ámbito subjetivo de la política de seguridad de este. También podrán contar con su propia política de seguridad, aprobada por el órgano competente, coherente con la del Departamento del que dependan o al que estén adscritos, los centros directivos de la propia Administración General del Estado que gestionen servicios bajo la declaración de servicios compartidos.
4. La Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital dispondrá de su propia política de seguridad, que será aprobada por la persona titular de la misma.
5. Los municipios podrán disponer de una política de seguridad común elaborada por la entidad local comarcal o provincial que asuma la responsabilidad de la seguridad de la información de los sistemas municipales.

6. La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de la actividad y detección de código dañino.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
ñ) Mejora continua del proceso de seguridad.

7. Los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos.

**Artículo 13.** *Organización e implantación del proceso de seguridad.*

1. La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.
2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

a) El responsable de la información determinará los requisitos de la información tratada
b) El responsable del servicio determinará los requisitos de los servicios prestados.
c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

3. El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.
4. Una Instrucción Técnica de Seguridad regulará el Esquema de Certificación de Responsables de la Seguridad, que recogerá las condiciones y requisitos exigibles a esta figura.
5. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

**Artículo 14.** *Análisis y gestión de los riesgos.*

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información o la prestación de servicios realizará su propia gestión de riesgos.
2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.
3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

**Artículo 15.** *Gestión de personal.*

1. El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.
2. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente.

**Artículo 16.** *Profesionalidad.*

1. La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.
2. Las entidades del ámbito de aplicación de este real decreto exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
3. Las organizaciones determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

**Artículo 17.** *Autorización y control de los accesos.*

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

**Artículo 18.** *Protección de las instalaciones.*

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

**Artículo 19.** *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

1. En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los

sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

2. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
b) Otras certificaciones de seguridad adicionales que se requieran normativamente.
c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

3. Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

**Artículo 20.** *Mínimo privilegio.*

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

**Artículo 21.** *Integridad y actualización del sistema.*

1. La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.
2. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

**Artículo 22.** *Protección de información almacenada y en tránsito.*

1. En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.
2. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.
3. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que

correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

**Artículo 23.** *Prevención ante otros sistemas de información interconectados.*

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

**Artículo 24.** *Registro de actividad y detección de código dañino.*

1. Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

3. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

**Artículo 25.** *Incidentes de seguridad.*

1. La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

**Artículo 26.** *Continuidad de la actividad.*

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

**Artículo 27.** *Mejora continua del proceso de seguridad.*

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

**Artículo 28.** *Cumplimiento de los requisitos mínimos.*

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:

a) Los activos que constituyen los sistemas de información concernidos.
b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.
c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Las medidas a las que se refiere el apartado 1 tendrán la condición de mínimos exigibles, siendo ampliables a criterio del responsable de la seguridad, quien podrá incluir medidas adicionales, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados. La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.

3. Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, del riesgo sobre los activos (anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III. Como parte integral de la Declaración de Aplicabilidad se indicará, de forma detallada, la correspondencia entre las medidas compensatorias implantadas y las medidas del anexo II que compensan. El conjunto será objeto de la aprobación formal por parte del responsable de la seguridad. Una Guía CCN-STIC de las previstas en la disposición adicional segunda guiará en la selección de dichas medidas, así como su registro e inclusión en la Declaración de Aplicabilidad.

**Artículo 29.** *Infraestructuras y servicios comunes.*

La utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto. Los supuestos concretos de utilización de estas infraestructuras y servicios serán determinados por cada administración pública.

**Artículo 30.** *Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras.*

1. En virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.

2. De forma análoga a lo dispuesto en el apartado anterior, para posibilitar la adecuada implantación y configuración de soluciones o plataformas suministradas por terceros, que vayan a ser usadas por las entidades comprendidas en el ámbito de aplicación de este real decreto, se podrán implementar esquemas de acreditación de entidades y validación de personas, que garanticen la seguridad de dichas soluciones o plataformas y la conformidad con lo dispuesto en este real decreto.

3. El CCN, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan y los antedichos esquemas de acreditación y validación, de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda.

4. Las correspondientes instrucciones técnicas de seguridad o, en su caso, las guías de Seguridad CCN-STIC, precisarán las condiciones a las que deberán sujetarse las implementaciones en modo local de productos, sistemas o servicios originariamente

prestados en la nube o en forma remota, así como las condiciones específicas para su evaluación y auditoría.

CAPÍTULO IV

**Seguridad de los sistemas: auditoría, informe e incidentes de seguridad**

**Artículo 31.** *Auditoría de la seguridad.*

1. Los sistemas de información comprendidos en el ámbito de aplicación de este real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

El plazo de dos años señalado en los párrafos anteriores podrá extenderse durante tres meses cuando concurran impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos.

2. La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

3. En la realización de las auditorías de la seguridad se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de actividades.

4. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto identificando los hallazgos de cumplimiento e incumplimiento detectados. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas, todo ello de conformidad con la citada Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

5. Los informes de auditoría serán presentados al responsable del sistema y al responsable de la seguridad. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

6. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, el responsable del sistema podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.

7. Los informes de auditoría podrán ser requeridos por los responsables de cada organización, con competencias sobre seguridad de las tecnologías de la información, y por el CCN.

**Artículo 32.** *Informe del estado de la seguridad.*

1. La Comisión Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere este real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las entidades titulares de los sistemas de información comprendidos en el ámbito de aplicación del artículo 2, que se plasmará en el informe correspondiente.

2. El CCN articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en la Comisión Sectorial de Administración Electrónica y en los órganos colegiados competentes en el ámbito de la Administración General del Estado.

3. Los resultados del informe serán utilizados por las autoridades competentes que impulsarán las medidas oportunas que faciliten la mejora continua del estado de la seguridad utilizando en su caso, cuadros de mando e indicadores que contribuyan a la toma de decisiones mediante el uso de las herramientas que el CCN provea para tal efecto.

**Artículo 33.** *Capacidad de respuesta a incidentes de seguridad.*

1. El CCN articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (por su acrónimo en inglés de *Computer Emergency Response Team),* que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

2. Sin perjuicio de lo establecido en el artículo 19.4 del Real Decreto-ley 12/2018, de 7 de septiembre, las entidades del sector público notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos, de acuerdo con la correspondiente Instrucción Técnica de Seguridad.

3. Cuando un operador esencial que haya sido designado como operador crítico sufra un incidente, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de su Oficina de Coordinación de Ciberseguridad, según lo previsto en el artículo 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. Cuando un operador con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, éste pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas, lo pondrá de inmediato en conocimiento de su CSIRT de referencia, quien informará a la capacidad de respuesta e incidentes de seguridad de referencia para el ámbito de la Defensa nacional, denominada ESPDEF-CERT, del Mando Conjunto del Ciberespacio (MCCE) a través de los canales establecidos. En estos casos, el ESPDEF-CERT del Mando Conjunto del Ciberespacio deberá ser oportunamente informado de la evolución de la gestión del incidente y podrá colaborar en la supervisión con la autoridad competente.

5. De conformidad con lo dispuesto en el Real Decreto-ley 12/2018, de 7 de septiembre, el CCN ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (denominados por su acrónimo en inglés *Computer Security Incident Response Team,* en adelante, CSIRT) en materia de seguridad de las redes y sistemas de información del sector público.

6. Tras un incidente de seguridad, el CCN-CERT determinará técnicamente el riesgo de reconexión del sistema o sistemas afectados, indicando los procedimientos a seguir y las salvaguardas a implementar con objeto de reducir el impacto para, en la medida de lo posible, evitar que vuelvan a darse las circunstancias que lo propiciaron.

Tras un incidente de seguridad, la Secretaría General de Administración Digital, sin perjuicio de la normativa que regula la continuidad de los sistemas de información implicados en la seguridad pública o la normativa que regule la continuidad de los sistemas de información militares implicados en la Defensa Nacional que requieran la participación del ESPDEF-CERT del Mando Conjunto del Ciberespacio, autorizará la reconexión a los medios y servicios comunes comprendidos bajo su ámbito de responsabilidad, incluidos los compartidos o transversales, si un informe de superficie de exposición del CCN-CERT hubiere determinado que el riesgo es asumible.

En caso de que se trate de un incidente de seguridad que afecte a un medio o servicio común bajo ámbito de responsabilidad de la Intervención General de la Administración del Estado, esta participará en el proceso de autorización de la reconexión a que se refiere el párrafo anterior.

7. Las organizaciones del sector privado que presten servicios a las entidades públicas notificarán al INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) dependiente del Ministerio de Asuntos Económicos y Transformación Digital, los incidentes que les afecten a través de su equipo de respuesta a incidentes de seguridad informática, quien, sin perjuicio de sus competencias y de lo previsto en los artículos 9, 10 y 11 del Real Decreto 43/2021, de

26 de enero, en relación con la Plataforma de Notificación y Seguimiento de Ciberincidentes, lo pondrá inmediatamente en conocimiento del CCN-CERT.

**Artículo 34.** *Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público.*

1. De acuerdo con lo previsto en el artículo 33, el CCN-CERT prestará los siguientes servicios:

a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las entidades del ámbito de aplicación de este real decreto.

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información afectados.

Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar informes, registros de auditoría y configuraciones de los sistemas afectados y cualquier otra información que se considere relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, sin perjuicio de lo dispuesto en la normativa de protección de datos que resulte de aplicación, así como de la posible confidencialidad de datos de carácter institucional u organizativo.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las entidades del sector público. Con esta finalidad, las series de documentos CCN-STIC (CCN-Seguridad de las Tecnologías de Información y la Comunicación), elaboradas por el CCN, ofrecerán normas, instrucciones, guías, recomendaciones y mejores prácticas para aplicar el ENS y para garantizar la seguridad de los sistemas de información del ámbito de aplicación de este real decreto.

c) Formación destinada al personal del sector público especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos y de lograr la sensibilización y mejora de sus capacidades para la prevención, detección y gestión de incidentes.

d) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las entidades del sector público puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquel, será coordinador a nivel público estatal.

## CAPÍTULO V

## Normas de conformidad

**Artículo 35.** *Administración digital.*

1. La seguridad de los sistemas de información que sustentan la administración digital se regirá por lo establecido en este real decreto.

*2.* El CCN es el órgano competente para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.

**Artículo 36.** *Ciclo de vida de servicios y sistemas.*

Las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

**Artículo 37.** *Mecanismos de control.*

Cada entidad titular de los sistemas de información comprendidos en el ámbito de aplicación de este real decreto y, en su caso, sus organismos, órganos, departamentos o

unidades, establecerán sus mecanismos de control para garantizar de forma real y efectiva el cumplimiento del ENS.

**Artículo 38.** *Procedimientos de determinación de la conformidad con el Esquema Nacional de Seguridad.*

1. Los sistemas de información comprendidos en el ámbito del artículo 2 serán objeto de un proceso para determinar su conformidad con el ENS. A tal efecto, los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad, sin perjuicio de la auditoría de la seguridad prevista en el artículo 31 que podrá servir asimismo para los fines de la certificación, mientras que los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, sin perjuicio de que se puedan someter igualmente a una auditoria de certificación.

Tanto el procedimiento de autoevaluación como la auditoría de certificación se realizarán según lo dispuesto en el artículo 31 y el anexo III y en los términos que se determinen en la correspondiente Instrucción Técnica de Seguridad, que concretará asimismo los requisitos exigibles a las entidades certificadoras.

2. Los sujetos responsables de los sistemas de información a que se refiere el apartado anterior darán publicidad, en los correspondientes portales de internet o sedes electrónicas a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la mencionada Instrucción Técnica de Seguridad.

## CAPÍTULO VI

## Actualización del Esquema Nacional de Seguridad

**Artículo 39.** *Actualización permanente.*

El ENS se mantendrá actualizado de manera permanente, desarrollándose y perfeccionándose a lo largo del tiempo, en paralelo al avance de los servicios prestados por las entidades del sector público, la evolución tecnológica, la aparición o consolidación de nuevos estándares internacionales sobre seguridad y auditoría y los riesgos a los que estén expuestos los sistemas de información concernidos.

## CAPÍTULO VII

## Categorización de los sistemas de información

**Artículo 40.** *Categorías de seguridad.*

1. La categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

2. La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I.

**Artículo 41.** *Facultades.*

1. La facultad para efectuar las valoraciones a las que se refiere el artículo 40, así como, en su caso, su posterior modificación, corresponderá al responsable o responsables de la información o servicios afectados.

2. Con base en las valoraciones señaladas en el apartado anterior, la determinación de la categoría de seguridad del sistema corresponderá al responsable o responsables de la seguridad.

**Disposición adicional primera.** *Formación.*

El CCN y el Instituto Nacional de Administración Pública desarrollarán programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público, para asegurar un adecuado despliegue de la información y las capacidades jurídicas, organizativas y técnicas relacionadas con la ciberseguridad de los sistemas de información públicos, y para garantizar el conocimiento permanente del ENS entre dichas entidades.

**Disposición adicional segunda.** *Desarrollo del Esquema Nacional de Seguridad.*

En desarrollo de lo dispuesto en este real decreto, la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante Resolución de dicha Secretaría de Estado.

Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas por la Unión Europea aplicables. Para su redacción y mantenimiento se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración digital.

Para el mejor cumplimiento de lo establecido en este real decreto, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.

**Disposición adicional tercera.** *Respeto del principio de «no causar un perjuicio significativo» al medioambiente.*

En cumplimiento con lo dispuesto en el Plan de Recuperación, Transformación y Resiliencia (PRTR) y en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, todas las actuaciones que se lleven a cabo en el marco del PRTR en cumplimiento del presente real decreto deben respetar el principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH por sus siglas en inglés, *Do No Significant Harm)* y las condiciones del etiquetado climático y digital.

**Disposición transitoria única.** *Adecuación de sistemas.*

1. Los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, incluidos aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2, dispondrán de veinticuatro meses para alcanzar su plena adecuación al ENS, circunstancia que se manifestará con la exhibición del correspondiente distintivo de conformidad, atendiendo lo dispuesto en el artículo 38.

2. Durante los antedichos veinticuatro meses, los sistemas de información preexistentes a la entrada en vigor de este real decreto que dispusieren de los correspondientes Distintivos de Conformidad, derivados de Declaraciones o Certificaciones de conformidad con el ENS, podrán mantener su vigencia procediendo a su renovación de conformidad y en los términos señalados por el Real Decreto 3/2010, de 8 de enero, del que trajeron causa.

3. Los nuevos sistemas de información aplicarán lo establecido en este real decreto desde su concepción.

**Disposición derogatoria única.** *Derogación normativa.*

Queda derogado el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como cuantas disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto.

**Disposición final primera.** *Títulos competenciales.*

Este real decreto se dicta en virtud de lo establecido en los artículos 149.1.18.ª, 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, las telecomunicaciones y la seguridad pública, respectivamente.

**Disposición final segunda.** *Desarrollo normativo.*

Se habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en este real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

**Disposición final tercera.** *Entrada en vigor.*

Este real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## ANEXO I

## Categorías de seguridad de los sistemas de información

*1. Fundamentos para la determinación de la categoría de seguridad de un sistema de información*

La determinación de la categoría de seguridad de un sistema de información se basará en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:

a) Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Garantizar la conformidad con el ordenamiento jurídico.

Anualmente, o siempre que se produzcan modificaciones significativas en los citados criterios de determinación, deberá re-evaluarse la categoría de seguridad de los sistemas de información concernidos.

*2. Dimensiones de la seguridad*

A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas:

a) Confidencialidad [C].
b) Integridad [I].
c) Trazabilidad [T].
d) Autenticidad [A].
e) Disponibilidad [D].

*3. Determinación del nivel de seguridad requerido en una dimensión de seguridad*

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles de seguridad: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel BAJO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

1.º La reducción de forma apreciable de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
2.º Causar un daño menor en los activos de la organización.
3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
4.º Causar un perjuicio menor a algún individuo, que pese a resultar molesto, pueda ser fácilmente reparable.
5.º Otros de naturaleza análoga.

b) Nivel MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio grave:

1.º La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
2.º Causar un daño significativo en los activos de la organización.
3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.
5.º Otros de naturaleza análoga.

c) Nivel ALTO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio muy grave:

1.º La anulación efectiva de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias.
2.º Causar un daño muy grave, e incluso irreparable, de los activos de la organización.
3.º El incumplimiento grave de alguna ley o regulación.
4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5.º Otros de naturaleza análoga.

Cuando un sistema de información trate diferentes informaciones y preste diferentes servicios, el nivel de seguridad del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

*4. Determinación de la categoría de seguridad de un sistema de información*

1. Se definen tres categorías de seguridad: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad ALTO.
b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO, y ninguna alcanza un nivel de seguridad superior.
c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

2. La determinación de la categoría de seguridad de un sistema de información sobre la base de lo indicado en el apartado anterior, no implicará que se altere, por este hecho, el nivel de seguridad de las dimensiones de seguridad que no han influido en la determinación de la categoría de seguridad del mismo.

*5. Secuencia de actuaciones para determinar la categoría de seguridad de un sistema*

1. Identificación del nivel de seguridad correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3 anterior.

2. Determinación de la categoría de seguridad del sistema, según lo establecido en el apartado 4 anterior.

Las guías CCN-STIC, del CCN, precisarán los criterios necesarios para una adecuada categorización de seguridad de los sistemas de información.

## ANEXO II

## Medidas de Seguridad

### *1. Disposiciones generales*

1. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

a) Las dimensiones de seguridad relevantes en el sistema a proteger.
b) La categoría de seguridad del sistema de información a proteger.

2. Las medidas de seguridad se dividen en tres grupos:

a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

### *2. Selección de medidas de seguridad*

1. Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

a) Identificación de los tipos de activos presentes.
b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.
c) Determinación del nivel de seguridad correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
d) Determinación de la categoría de seguridad del sistema, según lo establecido en el anexo I.
e) Selección de las medidas de seguridad, junto con los refuerzos apropiados, de entre las contenidas en este anexo, de acuerdo con las dimensiones y sus niveles de seguridad y para determinadas medidas de seguridad, de acuerdo con la categoría de seguridad del sistema.

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan subsistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad con los refuerzos correspondientes, y siempre que puedan delimitarse la información y los servicios afectados.

3. Las guías CCN-STIC, del CCN, podrán establecer perfiles de cumplimiento específicos, según el artículo 30 de este real decreto, para entidades o sectores concretos, que incluirán la relación de medidas y refuerzos que en cada caso resulten aplicables o los criterios para su determinación.

4. La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad con sus refuerzos, es la que se indica en la tabla siguiente:

| Medidas de Seguridad | | Por categoría o dimensión(es) | Nivel de las dimensiones de seguridad | | |
|---|---|---|---|---|---|
| | | | BAJO | MEDIO | ALTO |
| | | | Categoría de seguridad del sistema | | |
| | | | BÁSICA | MEDIA | ALTA |
| **org** | **Marco organizativo** | | | | |
| org.1 | Política de seguridad | Categoría | aplica | aplica | aplica |
| org.2 | Normativa de seguridad | Categoría | aplica | aplica | aplica |

| Medidas de Seguridad | | Por categoría o dimensión(es) | Nivel de las dimensiones de seguridad | | |
|---|---|---|---|---|---|
| | | | BAJO | MEDIO | ALTO |
| | | | Categoría de seguridad del sistema | | |
| | | | BÁSICA | MEDIA | ALTA |
| org.3 | Procedimientos de seguridad | Categoría | aplica | aplica | aplica |
| org.4 | Proceso de autorización | Categoría | aplica | aplica | aplica |
| **op** | **Marco operacional** | | | | |
| op.pl | Planificación | | | | |
| op.pl.1 | Análisis de riesgos | Categoría | aplica | + R1 | + R2 |
| op.pl.2 | Arquitectura de Seguridad | Categoría | aplica | + R1 | + R1 + R2 + R3 |
| op.pl.3 | Adquisición de nuevos componentes | Categoría | aplica | aplica | aplica |
| op.pl.4 | Dimensionamiento/gestión de la capacidad | D | aplica | + R1 | + R1 |
| op.pl.5 | Componentes certificados | Categoría | n.a. | aplica | aplica |
| op.acc | Control de acceso | | | | |
| op.acc.1 | Identificación | T A | aplica | + R1 | + R1 |
| op.acc.2 | Requisitos de acceso | C I T A | aplica | aplica | + R1 |
| op.acc.3 | Segregación de funciones y tareas | C I T A | n.a. | aplica | + R1 |
| op.acc.4 | Proceso de gestión de derechos de acceso | C I T A | aplica | aplica | aplica |
| op.acc.5 | Mecanismo de autenticación (usuarios externos) | C I T A | + [R1 o R2 o R3 o R4] | + [R2 o R3 o R4] + R5 | + [R2 o R3 o R4] + R5 |
| op.acc.6 | Mecanismo de autenticación (usuarios de la organización) | C I T A | + [R1 o R2 o R3 o R4] + R8 + R9 | + [R1 o R2 o R3 o R4] + R5 + R8 + R9 | + [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9 |
| op.exp | Explotación | | | | |
| op.exp.1 | Inventario de activos | Categoría | aplica | aplica | aplica |
| op.exp.2 | Configuración de seguridad | Categoría | aplica | aplica | aplica |
| op.exp.3 | Gestión de la configuración de seguridad | Categoría | aplica | + R1 | + R1 + R2 + R3 |
| op.exp.4 | Mantenimiento y actualizaciones de seguridad | Categoría | aplica | + R1 | + R1 + R2 |
| op.exp.5 | Gestión de cambios | Categoría | n.a. | aplica | + R1 |
| op.exp.6 | Protección frente a código dañino | Categoría | aplica | + R1 + R2 | + R1 + R2 + R3 + R4 |
| op.exp.7 | Gestión de incidentes | Categoría | aplica | + R1 + R2 | + R1 + R2 + R3 |
| op.exp.8 | Registro de la actividad | T | aplica | + R1 + R2 + R3 + R4 | + R1 + R2 + R3 + R4 + R5 |
| op.exp.9 | Registro de la gestión de incidentes | Categoría | aplica | aplica | aplica |
| op.exp.10 | Protección de claves criptográficas | Categoría | aplica | + R1 | + R1 |
| op.ext | Recursos externos | | | | |
| op.ext.1 | Contratación y acuerdos de nivel de servicio | Categoría | n.a. | aplica | aplica |
| op.ext.2 | Gestión diaria | Categoría | n.a. | aplica | aplica |
| op.ext.3 | Protección de la cadena de suministro | Categoría | n.a. | n.a. | aplica |
| op.ext.4 | Interconexión de sistemas | Categoría | n.a. | aplica | + R1 |
| op.nub | Servicios en la nube | | | | |
| op.nub.1 | Protección de servicios en la nube | Categoría | aplica | + R1 | + R1 + R2 |
| op.cont | Continuidad del servicio | | | | |
| op.cont.1 | Análisis de impacto | D | n.a. | aplica | aplica |
| op.cont.2 | Plan de continuidad | D | n.a. | n.a. | aplica |
| op.cont.3 | Pruebas periódicas | D | n.a. | n.a. | aplica |
| op.cont.4 | Medios alternativos | D | n.a. | n.a. | aplica |
| op.mon | Monitorización del sistema | | | | |
| op.mon.1 | Detección de intrusión | Categoría | aplica | + R1 | + R1 + R2 |
| op.mon.2 | Sistema de métricas | Categoría | aplica | + R1 + R2 | + R1 + R2 |
| op.mon.3 | Vigilancia | Categoría | aplica | + R1 + R2 | + R1 + R2 + R3 + R4 + R5 + R6 |
| mp | Medidas de protección | | | | |
| mp.if | Protección de las instalaciones e infraestructuras | | | | |
| mp.if.1 | Áreas separadas y con control de acceso | Categoría | aplica | aplica | aplica |
| mp.if.2 | Identificación de las personas | Categoría | aplica | aplica | aplica |
| mp.if.3 | Acondicionamiento de los locales | Categoría | aplica | aplica | aplica |
| mp.if.4 | Energía eléctrica | D | aplica | + R1 | + R1 |
| mp.if.5 | Protección frente a incendios | D | aplica | aplica | aplica |
| mp.if.6 | Protección frente a inundaciones | D | n.a. | aplica | aplica |
| mp.if.7 | Registro de entrada y salida de equipamiento | Categoría | aplica | aplica | aplica |
| mp.per | Gestión del personal | | | | |
| mp.per.1 | Caracterización del puesto de trabajo | Categoría | n.a. | aplica | aplica |
| mp.per.2 | Deberes y obligaciones | Categoría | aplica | + R1 | + R1 |
| mp.per.3 | Concienciación | Categoría | aplica | aplica | aplica |
| mp.per.4 | Formación | Categoría | aplica | aplica | aplica |
| mp.eq | Protección de los equipos | | | | |
| mp.eq.1 | Puesto de trabajo despejado | Categoría | aplica | + R1 | + R1 |
| mp.eq.2 | Bloqueo de puesto de trabajo | A | n.a. | aplica | + R1 |
| mp.eq.3 | Protección de dispositivos portátiles | Categoría | aplica | aplica | + R1 + R2 |
| mp.eq.4 | Otros dispositivos conectados a la red | C | aplica | + R1 | + R1 |
| mp.com | Protección de las comunicaciones | | | | |
| mp.com.1 | Perímetro seguro | Categoría | aplica | aplica | aplica |
| mp.com.2 | Protección de la confidencialidad | C | aplica | + R1 | + R1 + R2 + R3 |
| mp.com.3 | Protección de la integridad y de la autenticidad | I A | aplica | + R1 + R2 | + R1 + R2 + R3 + R4 |
| mp.com.4 | Separación de flujos de información en la red | Categoría | n.a. | + [R1 o R2 o R3] | + [R2 o R3] + R4 |
| mp.si | Protección de los soportes de información | | | | |
| mp.si.1 | Marcado de soportes | C | n.a. | aplica | aplica |
| mp.si.2 | Criptografía | C I | n.a. | aplica | + R1 + R2 |
| mp.si.3 | Custodia | Categoría | aplica | aplica | aplica |
| mp.si.4 | Transporte | Categoría | aplica | aplica | aplica |
| mp.si.5 | Borrado y destrucción | C | aplica | + R1 | + R1 |

| Medidas de Seguridad | | Por categoría o dimensión(es) | Nivel de las dimensiones de seguridad | | |
|---|---|---|---|---|---|
| | | | BAJO | MEDIO | ALTO |
| | | | Categoría de seguridad del sistema | | |
| | | | BÁSICA | MEDIA | ALTA |
| mp.sw | Protección de las aplicaciones informáticas | | | | |
| mp.sw.1 | Desarrollo de aplicaciones | Categoría | n.a. | + R1 + R2 + R3 + R4 | + R1 + R2 + R3 + R4 |
| mp.sw.2 | Aceptación y puesta en servicio | Categoría | aplica | + R1 | + R1 |
| mp.info | Protección de la información | | | | |
| mp.info.1 | Datos personales | Categoría | aplica | aplica | aplica |
| mp.info.2 | Calificación de la información | C | n.a. | aplica | aplica |
| mp.info.3 | Firma electrónica | I A | aplica | + R1 + R2 + R3 | + R1 + R2 + R3 + R4 |
| mp.info.4 | Sellos de tiempo | T | n.a. | n.a. | aplica |
| mp.info.5 | Limpieza de documentos | C | aplica | aplica | aplica |
| mp.info.6 | Copias de seguridad | D | aplica | + R1 | + R1 + R2 |
| mp.s | Protección de los servicios | | | | |
| mp.s.1 | Protección del correo electrónico | Categoría | aplica | aplica | aplica |
| mp.s.2 | Protección de servicios y aplicaciones web | Categoría | + [R1 o R2] | + [R1 o R2] | + R2 + R3 |
| mp.s.3 | Protección de la navegación web | Categoría | aplica | aplica | + R1 |
| mp.s.4 | Protección frente a denegación de servicio | D | n.a. | aplica | + R1 |

5. En las tablas del presente anexo se han empleado las siguientes convenciones:

a) La tercera columna indica si la medida se exige atendiendo al nivel de seguridad de una o más dimensiones de seguridad, o atendiendo a la categoría de seguridad del sistema. Cuando se exija por nivel de seguridad de las dimensiones, se indican cuales afectan utilizando sus iniciales.

b) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad, en algún nivel de seguridad determinado, se utiliza la voz «aplica».

c) «n.a.» significa «no aplica» a efectos de cumplimiento normativo, por lo que no es exigible, sin perjuicio de que su implantación en el sistema pudiera ser beneficioso técnicamente.

d) Para indicar una mayor exigencia se emplean los refuerzos de seguridad (R) que se suman (+) a los requisitos base de la medida pero que no siempre son incrementales entre sí.

e) Para señalar que se puede elegir entre aplicar un refuerzo u otro, se indicará entre corchetes y separados por «o» [Rn o Rn+1].

f) Se han empleado los colores verde, amarillo y rojo con el siguiente código: verde para indicar que una medida se aplica en sistemas de categoría BÁSICA o superior; el amarillo para indicar qué medidas y refuerzos empiezan a aplicar en categoría MEDIA o superior; y el rojo para indicar qué medidas o refuerzos son solo de aplicación en categoría ALTA o requieren un esfuerzo en seguridad superior al de categoría MEDIA.

6. A continuación, se describen individualmente cada una de las medidas organizadas de la siguiente forma:

a) Primero, una tabla resumen con las exigencias de seguridad de la medida en función de la categoría de seguridad del sistema y de las dimensiones de seguridad afectadas.

b) A continuación, una descripción con el cuerpo de la medida que desglosa los requisitos de base.

c) Posteriormente, podrán aparecer una serie de refuerzos adicionales que complementan a los requisitos de base, no en todos los casos requeridos o exigidos, y que podrían aplicarse en determinados perfiles de cumplimiento específicos.

d) Además, se indica el conjunto de requisitos y refuerzos exigidos en función de los niveles de seguridad o de la categoría de seguridad del sistema, según corresponda. En los casos en los que se pueda elegir entre aplicar un refuerzo u otro, además de indicarlo entre corchetes [Rm o Rn], se incluirá un diagrama de flujo explicativo.

e) Por último, algunos refuerzos son de carácter opcional, no siendo requeridos en todos los sistemas de información. Se aplicarán como medidas adicionales cuando el análisis de riesgos así lo recomiende.

*3. Marco organizativo [ORG]*

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1 Política de seguridad [org.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

La política de seguridad, que se aprobará de conformidad con lo dispuesto en el artículo 12 de este real decreto, se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente:

– [org.1.1] Los objetivos o misión de la organización.
– [org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades.
– [org.1.3] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
– [org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.
– [org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Aplicación de la medida.

– Categoría BÁSICA: org.1.
– Categoría MEDIA: org.1.
– Categoría ALTA: org.1.

3.2 Normativa de seguridad [org.2].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

Se dispondrá de una serie de documentos que describan:

– [org.2.1] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.
– [org.2.2] La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Refuerzo R1-Documentos específicos.

[org.2.r1.1] Se dispondrá de una documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación.

Aplicación de la medida.

– Categoría BÁSICA: org.2.
– Categoría MEDIA: org.2.
– Categoría ALTA: org.2.

3.3 Procedimientos de seguridad [org.3].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |

| | | | |
|---|---|---|---|
| | aplica | aplica | aplica |

Requisitos.

Se dispondrá de una serie de documentos que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

– [org.3.1] Cómo llevar a cabo las tareas habituales.
– [org.3.2] Quién debe hacer cada tarea.
– [org.3.3] Cómo identificar y reportar comportamientos anómalos.
– [org.3.4.] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:

a) Su control de acceso.
b) Su almacenamiento.
c) La realización de copias.
d) El etiquetado de soportes.
e) Su transmisión telemática.
f) Cualquier otra actividad relacionada con dicha información.

Refuerzo R1-Validación de procedimientos.

[org.3.r1.1] Se requerirá la validación de los procedimientos de seguridad por la autoridad correspondiente.

Aplicación de la medida.

– Categoría BÁSICA: org.3.
– Categoría MEDIA: org.3.
– Categoría ALTA: org.3.

3.4 Proceso de autorización [org.4].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos:

– [org.4.1] Utilización de instalaciones, habituales y alternativas.
– [org.4.2] Entrada de equipos en producción, en particular, equipos que involucren criptografía.
– [org.4.3] Entrada de aplicaciones en producción.
– [org.4.4] Establecimiento de enlaces de comunicaciones con otros sistemas.
– [org.4.5] Utilización de medios de comunicación, habituales y alternativos.
– [org.4.6] Utilización de soportes de información.
– [org.4.7] Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga.
– [org.4.8] Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.

Aplicación de la medida.

– Categoría BÁSICA: org.4.
– Categoría MEDIA: org.4.
– Categoría ALTA: org.4.

*4. Marco operacional [op]*

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1 | + R2 |

Requisitos.

Se realizará un análisis de riesgos informal, realizado en lenguaje natural. Es decir, una exposición textual que:

– [op.pl.1.1] Identifique los activos más valiosos del sistema. (Ver op.exp.1).
– [op.pl.1.2] Identifique las amenazas más probables.
– [op.pl.1.3] Identifique las salvaguardas que protegen de dichas amenazas.
– [op.pl.1.4] Identifique los principales riesgos residuales.

Refuerzo R1-Análisis de riesgos semiformal.

Se deberá realizar un análisis de riesgos semiformal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que:

– [op.pl.1.r1.1] Valore cualitativamente los activos más valiosos del sistema.
– [op.pl.1.r1.2] Cuantifique las amenazas más probables.
– [op.pl.1.r1.3] Valore las salvaguardas que protegen de dichas amenazas.
– [op.pl.1.r1.4] Valore el riesgo residual.

Refuerzo R2-Análisis de riesgos formal.

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente, que:

– [op.pl.1.r2.1] Valore cualitativamente los activos más valiosos del sistema.
– [op.pl.1.r2.2] Cuantifique las amenazas posibles.
– [op.pl.1.r2.3] Valore y priorice las salvaguardas adecuadas.
– [op.pl.1.r2.4] Valore y asuma formalmente el riesgo residual.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.1.
– Categoría MEDIA: op.pl.1 + R1.
– Categoría ALTA: op.pl.1 + R2.

4.1.2 Arquitectura de seguridad [op.pl.2].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1 | +R1+R2+R3 |

Requisitos.

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

– [op.pl.2.1] Documentación de las instalaciones, incluyendo áreas y puntos de acceso.
– [op.pl.2.2] Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración).
– [op.pl.2.3] Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de internet o redes públicas en general); cortafuegos, DMZ, etc.; y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

– [op.pl.2.4] Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga, y el uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Refuerzo R1-Sistema de gestión.

[op.pl.2.r1.1] Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Refuerzo R2-Sistema de gestión de la seguridad con mejora continua.

[op.pl.2.r2.1] Sistema de gestión de la seguridad de la información, con actualización y aprobación periódica.

Refuerzo R3-Validación de datos.

[op.pl.2.r3.1] Controles técnicos internos, incluyendo la validación de datos de entrada, salida y datos intermedios.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.2.
– Categoría MEDIA: op.pl.2 + R1.
– Categoría ALTA: op.pl.2 + R1 + R2 + R3.

4.1.3 Adquisición de nuevos componentes [op.pl.3].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

– [op.pl.3.1] Atenderá a las conclusiones del análisis de riesgos ([op.pl.1]).
– [op.pl.3.2] Será acorde a la arquitectura de seguridad escogida ([op.pl.2]).
– [op.pl.3.3] Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.3.
– Categoría MEDIA: op.pl.3.
– Categoría ALTA: op.pl.3.

4.1.4 Dimensionamiento / gestión de la capacidad [op.pl.4].

| dimensiones | D | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | + R1 | + R1 |

Requisitos.

Con carácter previo a la puesta en explotación, se realizará un estudio que cubrirá los siguientes aspectos:

– [op.pl.4.1] Necesidades de procesamiento.
– [op.pl.4.2] Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
– [op.pl.4.3] Necesidades de comunicación.
– [op.pl.4.4] Necesidades de personal: cantidad y cualificación profesional.
– [op.pl.4.5] Necesidades de instalaciones y medios auxiliares.

Refuerzo R1 –Mejora continua de la gestión de la capacidad.

– [op.pl.4.r1.1] Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema.
– [op.pl.4.r1.2] Se emplearán herramientas y recursos para la monitorización de la capacidad.

Aplicación de la medida (por disponibilidad):

– Nivel BAJO: op.pl.4.
– Nivel MEDIO: op.pl.4 + R1.
– Nivel ALTO: op.pl.4 + R1.

4.1.5 Componentes certificados [op.pl.5].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | n.a. | aplica | aplica |

Requisitos.

– [op.pl.5.1]. Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto.
En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.
Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.
– [op.pl.5.2] Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

Refuerzo R1-Protección de emisiones electromagnéticas.

[op.pl.5.r1.1] La información deberá ser protegida frente a las amenazas TEMPEST de acuerdo con la normativa en vigor.

Refuerzo R2 - Lista de componentes software.

[op.pl.5.r2.1] Cada producto y servicio incluirá en su descripción una lista de componentes software, acorde a lo especificado en [mp.sw.1.r5].

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.pl.5.
– Categoría ALTA: op.pl.5.

4.2 Control de acceso [op.acc].

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.
Los mecanismos de control de acceso deberán equilibrar la facilidad de uso y la protección de la información y los servicios, primando una u otra característica atendiendo a la categoría de seguridad del sistema.
Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se

acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).

4.2.1 Identificación [op.acc.1].

| dimensiones | T A | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | + R1 | + R1 |

Requisitos.

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

– [op.acc.1.1] Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

– [op.acc.1.2] Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

– [op.acc.1.3] Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.

– [op.acc.1.4] Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único.

b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó da orden en sentido contrario.

c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará «periodo de retención».

– [op.acc.1.5] En los supuestos de comunicaciones electrónicas, las partes intervinientes se identificarán atendiendo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE y sus normas de desarrollo o ejecución que resulten de aplicación:

a) Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

b) Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

c) Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento (UE) n.º 910/2014).

Refuerzo R1-Identificación avanzada.

– [op.acc.1.r1.1] La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.

– [op.acc.1.r1.2] Los datos de identificación serán utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad.
– [op.acc.1.r1.3] Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

Aplicación de la medida (por trazabilidad y autenticidad).

– Nivel BAJO: op.acc.1.
– Nivel MEDIO: op.acc.1 +R1.
– Nivel ALTO: op.acc.1+ R1.

4.2.2 Requisitos de acceso [op.acc.2].

| dimensiones | C I T A | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | aplica | + R1 |

Requisitos.

– [op.acc.2.1] Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.
– [op.acc.2.2] Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.
– [op.acc.2.3] Particularmente, se controlará el acceso a los componentes del sistema operativo y a sus ficheros o registros de configuración.

Refuerzo R1-Privilegios de acceso.

– [op.acc.2.r1.1] Todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.
– [op.acc.2.r1.2] Los privilegios de acceso se implementarán para restringir el tipo de acceso que un usuario puede tener (lectura, escritura, modificación, borrado, etc.).

Refuerzo R2-Control de acceso a dispositivos.

– [op.acc.2.r2.1] Se dispondrá de soluciones que permitan establecer controles de acceso a los dispositivos en función de la política de seguridad de la organización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.2.
– Nivel MEDIO: op.acc.2.
– Nivel ALTO: op.acc.2+ R1.

4.2.3 Segregación de funciones y tareas [op.acc.3].

| dimensiones | C I T A | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | aplica | + R1 |

Requisitos.

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita o no autorizada.

– [op.acc.3.1] Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona.
– [op.acc.3.2] Siempre que sea posible, las personas que autorizan y controlan el uso serán distintas.

Refuerzo R1-Segregación rigurosa.

– [op.acc.3.r1.1] Siempre que sea posible, la misma persona no aunará funciones de configuración y mantenimiento del sistema.
– [op.acc.3.r1.2] La misma persona no puede aunar funciones de auditoría o supervisión con cualquier otra función.

Refuerzo R2-Privilegios de auditoría.

– [op.acc.3.r2.1] Existirán cuentas con privilegios de auditoría estrictamente controladas y personalizadas.

Refuerzo R3-Acceso a la información de seguridad.

– [op.acc.3.r3.1] El acceso a la información de seguridad del sistema estará permitido únicamente a los administradores de seguridad/sistema autorizados, utilizando los mecanismos de acceso imprescindibles (consola, interfaz web, acceso remoto, etc.).

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: op.acc.3.
– Nivel ALTO: op.acc.3 + R1.

4.2.4 Proceso de gestión de derechos de acceso [op.acc.4].

| dimensiones | C I T A | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | aplica | aplica |

Requisitos.

Los derechos de acceso de cada entidad, usuario o proceso se limitarán atendiendo a los siguientes principios:

– [op.acc.4.1] Todo acceso estará prohibido, salvo autorización expresa.
– [op.acc.4.2] Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.
– [op.acc.4.3] Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.
– [op.acc.4.4] Capacidad de autorizar: Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica.
– [op.acc.4.5] Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

Nivel BAJO: op.acc.4.
Nivel MEDIO: op.acc.4.
Nivel ALTO: op.acc.4.

4.2.5 Mecanismo de autenticación (usuarios externos) [op.acc.5].

Referente a usuarios que no son usuarios de la organización.
Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

| dimensiones | C I T A |
|---|---|

| nivel | BAJO | MEDIO | ALTO |
|---|---|---|---|
| | + [R1 o R2 o R3 o R4] | + [R2 o R3 o R4] + R5 | + [R2 o R3 o R4] + R5 |

Requisitos.

– [op.acc.5.1] Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.
– [op.acc.5.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.
– [op.acc.5.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
– [op.acc.5.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.
– [op.acc.5.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.
– [op.acc.5.6] Las credenciales serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.
– [op.acc.5.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.
– [op.acc.5.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.
– [op.acc.5.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.5.r1.1] Se empleará una contraseña como mecanismo de autenticación.
– [op.acc.5.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + OTP.

– [op.acc.5.r2.1] Se requerirá una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario.

Refuerzo R3-Certificados.

– [op.acc.5.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.
– [op.acc.5.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.
– [op.acc.5.r3.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando un certificado electrónico cualificado.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.5.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.
– [op.acc.5.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

– [op.acc.5.r4.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando certificado electrónico cualificado.

Refuerzo R5-Registro.

– [op.acc.5.r5.1] Se registrarán los accesos con éxito y los fallidos.
– [op.acc.5.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.5.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.5.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.5 + [R1 o R2 o R3 o R4].
– Nivel MEDIO: op.acc.5 + [R2 o R3 o R4] + R5.
– Nivel ALTO: op.acc.5 + [R2 o R3 o R4] + R5.

4.2.6 Mecanismo de autenticación (usuarios de la organización) [op.acc.6].

Esta medida se refiere a personal del organismo, propio o contratado, estable o circunstancial, que pueda tener acceso a información contenida en el sistema.

Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación, en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

| dimensiones | C I T A | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | + [R1 o R2 o R3 o R4] + R8 + R9 | + [R1 o R2 o R3 o R4] + R5 + R8 + R9 | + [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9 |

Requisitos.

– [op.acc.6.1] Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten.
– [op.acc.6.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que ha recibido las credenciales de acceso y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.
– [op.acc.6.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
– [op.acc.6.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.
– [op.acc.6.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.
– [op.acc.6.6] Las credenciales serán inhabilitadas cuando el usuario que autentican termina su relación con el sistema.
– [op.acc.6.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

– [op.acc.6.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.
– [op.acc.6.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.6.r1.1] Se empleará una contraseña como mecanismo de autenticación cuando el acceso se realiza desde zonas controladas y sin atravesar zonas no controladas (véase refuerzo R8).
– [op.acc.6.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + otro factor de autenticación.

– [op.acc.6.r2.1] Se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es».

Refuerzo R3-Certificados.

– [op.acc.6.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.
– [op.acc.6.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.6.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.
– [op.acc.6.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R5-Registro.

– [op.acc.6.r5.1] Se registrarán los accesos con éxito y los fallidos.
– [op.acc.6.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.6.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.6.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Refuerzo R8-Doble factor para acceso desde o a través de zonas no controladas.

Se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet.

– [op.acc.6.r8.1] Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación: R2, R3 o R4.

Refuerzo R9-Acceso remoto (todos los niveles).

– [op.acc.6.r9.1] Será de aplicación la ITS de Interconexión de sistemas de información.
– [op.acc.6.r9.2] El acceso remoto deberá considerar los siguientes aspectos:

a) Ser autorizado por la autoridad correspondiente.
b) El tráfico deberá ser cifrado.

c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario.
d) Deberán recogerse registros de auditoría de este tipo de conexiones.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.6 + [R1 o R2 o R3 o R4] + R8 + R9.
– Nivel MEDIO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R8 + R9.
– Nivel ALTO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9.

4.3 Explotación [op.exp].

4.3.1 Inventario de activos [op.exp.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

[op.exp.1.1] Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que toma las decisiones relativas al mismo.

Refuerzo R1-Inventario de etiquetado.

– [op.exp.1.r1.1] El etiquetado del equipamiento y del cableado formará parte del inventario.

Refuerzo R2-Identificación periódica de activos.

– [op.exp.1.r2.1] Se dispondrá de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, en particular, los servidores y los dispositivos de red y de comunicaciones.

Refuerzo R3-Identificación de activos críticos.

– [op.exp.1.r3.1] Se dispondrá de herramientas que permitan categorizar los activos críticos por contexto de la organización y riesgos de seguridad.

Refuerzo R4-Lista de componentes software.

– [op.exp.1.r4.1] Se mantendrá actualizada una relación formal de los componentes software de terceros empleados en el despliegue del sistema. Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional). El contenido de la lista de componentes será equivalente a lo requerido en [mp.sw.1.r5].

Aplicación de la medida.

– Categoría BÁSICA: op.exp.1.
– Categoría MEDIA: op.exp.1.
– Categoría ALTA: op.exp.1.

4.3.2 Configuración de seguridad [op.exp.2].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

Se configurarán los equipos previamente a su entrada en operación, de forma que:

– [op.exp.2.1] Se retiren cuentas y contraseñas estándar.
– [op.exp.2.2] Se aplicará la regla de «mínima funcionalidad», es decir:

a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos.
b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.

– [op.exp.2.3] Se aplicará la regla de «seguridad por defecto», es decir:

a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
b) Para reducir la seguridad, el usuario tendrá que realizar acciones conscientes.
c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

– [op.exp.2.4] Las máquinas virtuales estarán configuradas y gestionadas de un modo seguro. La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.2.
– Categoría MEDIA: op.exp.2.
– Categoría ALTA: op.exp.2.

4.3.3 Gestión de la configuración de seguridad [op.exp.3].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1 | +R1+R2+R3 |

Requisitos.

Se gestionará de forma continua la configuración de los componentes del sistema, de forma que:

– [op.exp.3.1] Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).
– [op.exp.3.2] Se mantenga en todo momento la regla de "mínimo privilegio" ([op.exp.2]).
– [op.exp.3.3] El sistema se adapte a las nuevas necesidades, previamente autorizadas. (Ver [op.acc.4]).
– [op.exp.3.4] El sistema reaccione a vulnerabilidades notificadas. (Ver [op.exp.4]).
– [op.exp.3.5] El sistema reaccione a incidentes. (Ver [op.exp.7]).
– [op.exp.3.6] La configuración de seguridad solamente podrá editarse por personal debidamente autorizado.

Refuerzo R1-Mantenimiento regular de la configuración.

– [op.exp.3.r1.1] Existirán configuraciones hardware/software, autorizadas y mantenidas regularmente, para los servidores, elementos de red y estaciones de trabajo.
– [op.exp.3.r1.2] Se verificará periódicamente la configuración hardware/software del sistema para asegurar que no se han introducido ni instalado elementos no autorizados.
– [op.exp.3.r1.3] Se mantendrá una lista de servicios autorizados para servidores y estaciones de trabajo.

Refuerzo R2-Responsabilidad de la configuración.
– [op.exp.3.r2.1] La configuración de seguridad del sistema operativo y aplicaciones, tanto de estaciones y servidores como de la electrónica de red del sistema, será responsabilidad de un número muy limitado de administradores del sistema.

Refuerzo R3-Copias de seguridad.

– [op.exp.3.r3.1] Se realizarán copias de seguridad de la configuración del sistema de forma que sea posible reconstruirlo en parte o en su totalidad tras un incidente.

Refuerzo R4-Aplicación de la configuración.

– [op.exp.3.r4.1] La configuración de seguridad del sistema operativo y de las aplicaciones se mantendrá actualizada a través de una aplicación o procedimiento manual que permita la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas.

Refuerzo R5-Control del estado de seguridad de la Configuración.

– [op.exp.3.r5.1] Se dispondrá de herramientas que permitan conocer de forma periódica el estado de seguridad de la configuración de los dispositivos de red y, en el caso de que resulte deficiente, permitir su corrección.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.3.
– Categoría MEDIA: op.exp.3 + R1.
– Categoría ALTA: op.exp.3 + R1 + R2 + R3.

4.3.4 Mantenimiento y actualizaciones de seguridad [op.exp.4].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1 | +R1+R2 |

Requisitos.

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

– [op.exp.4.1] Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.
– [op.exp.4.2] Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.
– [op.exp.4.3] El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Refuerzo R1-Pruebas en preproducción.

[op.exp.4.r1.1] Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

Refuerzo R2-Prevención de fallos.

[op.exp.4.r2.1] Antes de la aplicación de las configuraciones, parches y actualizaciones de seguridad se preverá un mecanismo para revertirlos en caso de aparición de efectos adversos.

Refuerzo R3-Actualizaciones y pruebas periódicas.

[op.exp.4.r3.1] Se deberá comprobar de forma periódica la integridad del firmware utilizado en los dispositivos hardware del sistema (infraestructura de red, BIOS, etc.). La periodicidad de estas comprobaciones seguirá las recomendaciones de la Guía CCN-STIC que sea de aplicación.

Refuerzo R4 - Monitorización continua.

[op.exp.4.r4.1] Se desplegará a nivel de sistema una estrategia de monitorización continua de amenazas y vulnerabilidades. Esta estrategia detallará:

1. Los indicadores críticos de seguridad a emplear.

2. La política de aplicación de parches de seguridad de los componentes software relacionados en las listas de [op.exp.1.r4], [op.ext.3.r3] y [mp.sw.1.r5]).
3. Los criterios de revisión regular y excepcional de las amenazas sobre el sistema.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.4.
– Categoría MEDIA: op.exp.4 + R1.
– Categoría ALTA: op.exp.4 + R1 + R2.

4.3.5 Gestión de cambios [op.exp.5].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | n.a. | aplica | + R1 |

Requisitos.

Se mantendrá un control continuo de los cambios realizados en el sistema, de forma que:

– [op.exp.5.1] Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. Para ello, todas las peticiones de cambio se registrarán asignando un número de referencia que permita su seguimiento, de forma equivalente al registro de los incidentes.
– [op.exp.5.2] La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.
– [op.exp.5.3] Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.
– [op.exp.5.4] Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO deberán ser aprobados, explícitamente, de forma previa a su implantación, por el Responsable de la Seguridad.
– [op.exp.5.5] Una vez implementado el cambio, se realizarán las pruebas de aceptación convenientes. Si son positivas, se actualizará la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda.

Refuerzo R1-Prevención de fallos.

– [op.exp.5.r1.1] Antes de la aplicación de los cambios, se deberá tener en cuenta la posibilidad de revertirlos en caso de la aparición de efectos adversos.
– [op.exp.5.r1.2] Todos los fallos en el software y hardware deberán ser comunicados al responsable designado en la organización de la seguridad.
– [op.exp.5.r1.3] Todos los cambios en el sistema deberán documentarse, incluyendo una valoración del impacto que dicho cambio supone en la seguridad del sistema.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.exp.5.
– Categoría ALTA: op.exp.5+ R1.

4.3.6 Protección frente a código dañino [op.exp.6].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1+R2 | +R1+R2+R3+R4 |

Requisitos.

– [op.exp.6.1] Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante.
– [op.exp.6.2] Se instalará software de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales.
– [op.exp.6.3] Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.
– [op.exp.6.4] Las bases de datos de detección de código dañino permanecerán permanentemente actualizadas.
– [op.exp.6.5] El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Refuerzo R1-Escaneo periódico.

– [op.exp.6.r1.1] Todo el sistema se escaneará regularmente para detectar código dañino.

Refuerzo R2-Revisión preventiva del sistema.

– [op.exp.6.r2.1] Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.

Refuerzo R3 - Lista blanca.

– [op.exp.6.r3.1] Solamente se podrán ejecutar aquellas aplicaciones previamente autorizadas. Se implementará una lista blanca para impedir la ejecución de aplicaciones no autorizadas.

Refuerzo R4-Capacidad de respuesta en caso de incidente.

– [op.exp.6.r4.1] Se emplearán herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - *Endpoint Detection and Response*).

Refuerzo R5-Configuración de la herramienta de detección de código dañino.

– [op.exp.6.r5.1] El software de detección de código dañino permitirá realizar configuraciones avanzadas y revisar el sistema en el arranque y cada vez que se conecte un dispositivo extraíble.
– [op.exp.6.r5.2] El software de detección de código dañino instalado en servidores y elementos perimetrales deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.6.
– Categoría MEDIA: op.exp.6+ R1 + R2.
– Categoría ALTA: op.exp.6+ R1 + R2 + R3 + R4.

4.3.7 Gestión de incidentes [op.exp.7].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1+R2 | + R1+R2+ R3 |

Requisitos.

– [op.exp.7.1] Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.
– [op.exp.7.2] La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5

de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto.

Refuerzo R1-Notificación.

– [op.exp.7.r1.1] Se dispondrá de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.

Refuerzo R2 –Detección y Respuesta.

El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema ([op.exp.7.1]) deberá incluir:

– [op.exp.7.r2.1] Implantación de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
– [op.exp.7.r2.2] Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
– [op.exp.7.r2.3] Informar del incidente a los responsables de la información y servicios afectados y de las actuaciones llevadas a cabo para su resolución.
– [op.exp.7.r2.4] Medidas para:

a) Prevenir que se repita el incidente.
b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

Refuerzo R3-Reconfiguración dinámica.

La reconfiguración dinámica del sistema persigue detener, desviar o limitar ataques, acotando los daños.
– [op.exp.7.r3.1] La reconfiguración dinámica incluye, por ejemplo, cambios en las reglas de los enrutadores (*routers*), listas de control de acceso, parámetros del sistema de detección / prevención de intrusiones y reglas en los cortafuegos y puertas de enlace, aislamiento de elementos críticos y aislamiento de las copias de seguridad.
– [op.exp.7.r3.2] El organismo adaptará los procedimientos de reconfiguración dinámica reaccionando a los anuncios recibidos del CCN-CERT relativos a ciberamenazas sofisticadas y campañas de ataques.

Refuerzo R4-Prevención y Respuesta Automática.

– [op.exp.7.r4.1] Se dispondrá de herramientas que automaticen el proceso de prevención y respuesta mediante la detección e identificación de anomalías, la segmentación dinámica de la red para reducir la superficie de ataque, el aislamiento de dispositivos críticos, etc.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.7.
– Categoría MEDIA: op.exp.7+ R1 + R2.
– Categoría ALTA: op.exp.7+ R1 + R2 + R3.

4.3.8 Registro de la actividad [op.exp.8].

| dimensiones | T | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | +R1+R2+R3+R4 | +R1+R2+R3+R4+R5 |

Requisitos.

Se registrarán las actividades en el sistema, de forma que:

– [op.exp.8.1] Se generará un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma.
– [op.exp.8.2] Se activarán los registros de actividad en los servidores.

Refuerzo R1-Revisión de los registros.

– [op.exp.8.r1.1] Se revisarán informalmente, de forma periódica, los registros de actividad, buscando patrones anormales.

Refuerzo R2-Sincronización del reloj del sistema.

– [op.exp.8.r2.1] El sistema deberá disponer de una referencia de tiempo (*timestamp*) para facilitar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.

Refuerzo R3-Retención de registros.

– [op.exp.8.r3.1] En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados.

Refuerzo R4-Control de acceso.

– [op.exp.8.r4.1] Los registros de actividad y, en su caso, las copias de seguridad de los mismos, solamente podrán ser accedidos o eliminarse por personal debidamente autorizado.

Refuerzo R5-Revisión automática y correlación de eventos.

– [op.exp.8.r5.1] El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales.
– [op.exp.8.r5.2] Se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

Aplicación de la medida (por trazabilidad).

– Nivel BAJO: op.exp.8.
– Nivel MEDIO: op.exp.8 + R1 + R2 + R3 + R4.
– Nivel ALTO: op.exp.8 + R1 + R2 + R3 + R4 + R5.

4.3.9 Registro de la gestión de incidentes [op.exp.9].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

– [op.exp.9.1] Se registrarán los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.
– [op.exp.9.2] Se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.
– [op.exp.9.3] Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.9.
– Categoría MEDIA: op.exp.9.
– Categoría ALTA: op.exp.9.

4.3.10 Protección de claves criptográficas [op.exp.10].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1 | + R1 |

Requisitos.

– [op.exp.10.1] Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.
– [op.exp.10.2] Los medios de generación estarán aislados de los medios de explotación.
– [op.exp.10.3] Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Refuerzo R1-Algoritmos autorizados.

– [op.exp.10.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Protección avanzada de claves criptográficas.

– [op.exp.10.r2.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.10.
– Categoría MEDIA: op.exp.10 + R1.
– Categoría ALTA: op.exp.10 + R1.

4.4 Recursos externos [op.ext].

Cuando la organización utilice recursos externos (servicios, productos, instalaciones o personal), mantendrá la plena responsabilidad de los riesgos para la información tratada o los servicios prestados, debiendo adoptar las medidas necesarias para ejercer su responsabilidad y mantener el control en todo momento.

4.4.1 Contratación y acuerdos de nivel de servicio [op.ext.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | n.a. | aplica | aplica |

Requisitos.

– [op.ext.1.1] Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como «servicio mínimo admisible», así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.1.
– Categoría ALTA: op.ext.1.

4.4.2 Gestión diaria [op.ext.2].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | n.a. | aplica | aplica |

Requisitos.

Se establecerá lo siguiente:

– [op.ext.2.1] Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).
– [op.ext.2.2] El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres (ver [op.exp.7]).

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.2.
– Categoría ALTA: op.ext.2.

4.4.3 Protección de la cadena de suministro [op.ext.3].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | n.a. | n.a. | aplica |

Requisitos.

– [op.ext.3.1] Se analizará el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro.
– [op.ext.3.2] Se estimará el riesgo sobre el sistema por causa del impacto estimado en el punto anterior.
– [op.ext.3.3] Se tomarán medidas de contención de los impactos estimados en los puntos anteriores.

Refuerzo R1-Plan de contingencia.

– [op.ext.3.r1.1] El plan de continuidad de la organización deberá tener en cuenta la dependencia de proveedores externos críticos.
– [op.ext.3.r1.2] Se deberán realizar pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor.

Refuerzo R2-Sistema de gestión de la seguridad.

– [op.ext.3.r2.1] Se implementará un sistema de protección de los procesos y flujos de información en las relaciones en línea (*online*) entre los distintos integrantes de la cadena de suministro.

Refuerzo R3-Lista de componentes software.

– [op.ext.3.r3.1] Se mantendrá actualizado un registro formal que contenga los detalles y las relaciones de la cadena de suministro de los diversos componentes utilizados en la construcción de programas informáticos, acorde a lo especificado en [mp.sw.1.r5]. Esta lista será proporcionada por el proveedor de la aplicación, librería o producto suministrado.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: no aplica.
– Categoría ALTA: op.ext.3.

4.4.4 Interconexión de sistemas [op.ext.4].

Se denomina interconexión al establecimiento de enlaces con otros sistemas de información para el intercambio de información y servicios.

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | n.a. | aplica | + R1 |

Requisitos.

– [op.ext.4.1] Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.
– [op.ext.4.2] Para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.

Refuerzo R1-Coordinación de actividades.

– [op.ext.4.r1.1] Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, las medidas de seguridad locales se acompañarán de los correspondientes mecanismos y procedimientos de coordinación para la atribución y ejercicio efectivos de las responsabilidades de cada sistema.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.4.
– Categoría ALTA: op.ext.4 + R1.

4.5 Servicios en la nube [op.nub].

4.5.1 Protección de servicios en la nube [op.nub.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1 | +R1+R2 |

Requisitos.

– [op.nub.1.1] Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (*Software as a Service, SaaS*), Plataforma como Servicio (*Platform as a Service, PaaS*) e Infraestructura como Servicio (*Infrastructure as a Service, IaaS*) definidas en las guías CCN-STIC que sean de aplicación.
– [op.nub.1.2] Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

a) Auditoría de pruebas de penetración (*pentesting*).
b) Transparencia.
c) Cifrado y gestión de claves.
d) Jurisdicción de los datos.

Refuerzo R1- Servicios certificados.

– [op.nub.1.r1.1] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.
– [op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

Refuerzo R2-Guías de Configuración de Seguridad Específicas.

– [op.nub.1.r2.1] La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.

Aplicación de la medida.

– Categoría BÁSICA: op.nub.1.
– Categoría MEDIA: op.nub.1 + R1.
– Categoría ALTA: op.nub.1+ R1 + R2.

4.6 Continuidad del servicio [op.cont].

4.6.1 Análisis de impacto [op.cont.1].

| dimensiones | D | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | aplica | aplica |

Requisitos.

– [op.cont.1.1] Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: op.cont.1.
– Nivel ALTO: op.cont.1.

4.6.2 Plan de continuidad [op.cont.2].

| dimensiones | D | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | n.a. | aplica |

Requisitos.

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan contemplará los siguientes aspectos:

– [op.cont.2.1] Se identificarán funciones, responsabilidades y actividades a realizar.
– [op.cont.2.2] Existirá una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización.
– [op.cont.2.3] Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
– [op.cont.2.4] Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
– [op.cont.2.5] El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

Refuerzo R1-Plan de emergencia y contingencia.

– [op.cont.2.r1.1] Cuando se determine la necesidad de continuidad de los sistemas, deberá existir un plan de emergencia y contingencia en consonancia. En función del análisis de Impacto, se determinarán los aspectos a cubrir.

Refuerzo R2-Comprobación de integridad.

– [op.cont.2.r2.1] Ante una caída o discontinuidad del sistema, se deberá comprobar la integridad del sistema operativo, del firmware y de los ficheros de configuración.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.2.

4.6.3 Pruebas periódicas [op.cont.3].

| dimensiones | D | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | n.a. | aplica |

Requisitos.

– [op.cont.3.1] Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.3.

4.6.4 Medios alternativos [op.cont.4].

| dimensiones | D | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | n.a. | aplica |

Requisitos.

– [op.cont.4.1] Estará prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto, se cubrirán los siguientes elementos del sistema:

a) Servicios contratados a terceros.
b) Instalaciones alternativas.
c) Personal alternativo.
d) Equipamiento informático alternativo.
e) Medios de comunicación alternativos.

– [op.cont.4.2] Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento.
– [op.cont.4.3] Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales.

Refuerzo R1-Automatización de la transición a medios alternativos.

– [op.cont.4.r1.1] El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.4.

4.7 Monitorización del sistema [op.mon].

El sistema estará sujeto a medidas de monitorización de su actividad y ejecutará acciones predeterminadas en función de las situaciones de compromiso de la seguridad que figuren en el análisis de riesgos. Esto puede incluir la generación de alarmas en tiempo real, la finalización del proceso que está ocasionando la alarma, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

4.7.1 Detección de intrusión [op.mon.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1 | +R1+R2 |

Requisitos.

– [op.mon.1.1] Se dispondrá de herramientas de detección o prevención de intrusiones.

Refuerzo R1-Detección basada en reglas.

– [op.mon.1.r1.1] El sistema dispondrá de herramientas de detección o prevención de intrusiones basadas en reglas.

Refuerzo R2-Procedimientos de respuesta.

– [op.mon.1.r2.1] Existirán procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones.

Refuerzo R3-Acciones predeterminadas.

– [op.mon.1.r3.1] El sistema ejecutará automáticamente acciones predeterminadas de respuesta a las alertas generadas. Esto puede incluir la finalización del proceso que está ocasionando la alerta, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.1.
– Categoría MEDIA: op.mon.1 + R1.
– Categoría ALTA: op.mon.1+ R1 + R2.

4.7.2 Sistema de métricas [op.mon.2].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1+R2 | + R1+R2 |

Requisitos.

– [op.mon.2.1] Atendiendo a la categoría de seguridad del sistema, se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables y, en su caso, para proveer el informe anual requerido por el artículo 32.

Refuerzo R1-Efectividad del sistema de gestión de incidentes.

– [op.mon.2.r1.1] Se recopilarán los datos precisos que posibiliten evaluar el comportamiento del sistema de gestión de incidentes, de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y con la correspondiente guía CCN-STIC.

Refuerzo R2-Eficiencia del sistema de gestión de la seguridad.

– [op.mon.2.r2.1] Se recopilarán los datos precisos para conocer la eficiencia del sistema de seguridad, en relación con los recursos consumidos, en términos de horas y presupuesto.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.2.
– Categoría MEDIA: op.mon.2 + R1+ R2.
– Categoría ALTA: op.mon.2 + R1 + R2.

4.7.3 Vigilancia [op.mon.3].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |

| | aplica | + R1+R2 | + R1+R2+R3+R4+R5+R6 |
|---|---|---|---|

Requisitos.

– [op.mon.3.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad.

Refuerzo R1-Correlación de eventos.

– [op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

Refuerzo R2-Análisis dinámico.

– [op.mon.3.r2.1] Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

Refuerzo R3-Ciberamenazas avanzadas.

– [op.mon.3.r3.1] Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos.
– [op.mon.3.r3.2] Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (*Advanced Persistent Threat, APT*) mediante la detección de anomalías significativas en el tráfico de la red.

Refuerzo R4-Observatorios digitales.

– [op.mon.3.r4.1] Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías que pudieran representar indicadores de amenaza en contenidos digitales.

Refuerzo R5-Minería de datos.

Se aplicarán medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos:

– [op.mon.3.r5.1] Limitación de las consultas, monitorizando volumen y frecuencia.
– [op.mon.3.r5.2] Alerta a los administradores de seguridad de comportamientos sospechosos en tiempo real.

Refuerzo R6-Inspecciones de seguridad.

Periódicamente, o tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas, se realizarán las siguientes inspecciones:

– [op.mon.3.r6.1] Verificación de configuración.
– [op.mon.3.r6.2] Análisis de vulnerabilidades.
– [op.mon.3.r6.3] Pruebas de penetración.

Refuerzo R7-Interconexiones.

– [op.mon.3.r7.1] En las interconexiones que lo requieran se aplicarán controles en los flujos de intercambio de información a través del uso de metadatos.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.3.
– Categoría MEDIA: op.mon.3 + R1 + R2.
– Categoría ALTA: op.mon.3 + R1 + R2 + R3 + R4 + R5 + R6.

*5. Medidas de protección [mp]*

Las medidas de protección estarán dirigidas a proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

5.1 Protección de las instalaciones e infraestructuras [mp.if].

5.1.1 Áreas separadas y con control de acceso [mp.if.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

– [mp.if.1.1] El equipamiento del Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas, específicas para su función.
– [mp.if.1.2] Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.1.
– Categoría MEDIA: mp.if.1.
– Categoría ALTA: mp.if.1.

5.1.2 Identificación de las personas [mp.if.2].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

[mp.if.2.1] El procedimiento de control de acceso identificará a las personas que accedan a los locales donde hay equipamiento esencial que forme parte del sistema de información del CPD, registrando las correspondientes entradas y salidas.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.2.
– Categoría MEDIA: mp.if.2.
– Categoría ALTA: mp.if.2.

5.1.3 Acondicionamiento de los locales [mp.if.3].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado, y, en especial, para asegurar:

– [mp.if.3.1] Las condiciones de temperatura y humedad.
– [mp.if.3.2] La protección frente a las amenazas identificadas en el análisis de riesgos.
– [mp.if.3.3] La protección del cableado frente a incidentes fortuitos o deliberados.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.3.
– Categoría MEDIA: mp.if.3.
– Categoría ALTA: mp.if.3.

5.1.4 Energía eléctrica [mp.if.4].

| dimensiones | D | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | + R1 | + R1 |

Requisitos.

– [mp.if.4.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de tomas de energía eléctrica, de modo que se garantice el suministro y el correcto funcionamiento de las luces de emergencia.

Refuerzo R1-Suministro eléctrico de emergencia.

– [mp.if.4.r1.1] En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: mp.if.4.
– Nivel MEDIO: mp.if.4 + R1.
– Nivel ALTO: mp.if.4 + R1.

5.1.5 Protección frente a incendios [mp.if.5].

| dimensiones | D | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | aplica | aplica |

Requisitos.

– [mp.if.5.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incendios atendiendo, al menos, a la normativa industrial de aplicación.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: mp.if.5.
– Nivel MEDIO: mp.if.5.
– Nivel ALTO: mp.if.5.

5.1.6 Protección frente a inundaciones [mp.if.6].

| dimensiones | D | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | aplica | aplica |

Requisitos.

– [mp.if.6.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.if.6.
– Nivel ALTO: mp.if.6.

5.1.7 Registro de entrada y salida de equipamiento [mp.if.7].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

– [mp.if.7.1] Se llevará un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.7.
– Categoría MEDIA: mp.if.7.
– Categoría ALTA: mp.if.7.

5.2 Gestión del personal [mp.per].

5.2.1 Caracterización del puesto de trabajo [mp.per.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | n.a. | aplica | aplica |

Requisitos.

– [mp.per.1.1] Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, se definirán las responsabilidades en materia de seguridad, que estarán basadas en el análisis de riesgos.
– [mp.per.1.2] Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar el puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias, de conformidad con el ordenamiento jurídico y el respeto a los derechos fundamentales.

Refuerzo R1-Habilitación Personal de Seguridad.

– [mp.per.1.r1.1] Los administradores de seguridad/sistema tendrán una Habilitación Personal de Seguridad (HPS) otorgada por la autoridad competente, como consecuencia de los resultados del análisis de riesgos previo o como requisito de seguridad de un sistema específico.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.per.1.
– Categoría ALTA: mp.per.1.

5.2.2 Deberes y obligaciones [mp.per.2].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1 | + R1 |

Requisitos.

Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, contemplando:

– [mp.per.2.1] Las medidas disciplinarias a que haya lugar.
– [mp.per.2.2] Contemplando tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
– [mp.per.2.3] El deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.
– [mp.per.2.4] En caso de personal contratado a través de un tercero:

• [mp.per.2.4.1] Se establecerán los deberes y obligaciones de cada parte y del personal contratado.
• [mp.per.2.4.2] Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Refuerzo R1-Confirmación expresa.

– [mp.per.2.r1.1] Se ha de obtener la confirmación expresa de que los usuarios conocen las instrucciones de seguridad necesarias y obligatorias y su aceptación, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.2.
– Categoría MEDIA: mp.per.2 + R1.
– Categoría ALTA: mp.per.2 + R1.

5.2.3 Concienciación [mp.per.3].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente:

– [mp.per.3.1] La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
– [mp.per.3.2] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
– [mp.per.3.3] El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.3.
– Categoría MEDIA: mp.per.3.
– Categoría ALTA: mp.per.3.

5.2.4 Formación [mp.per.4].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

– [mp.per.4.1] Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:

a) Configuración de sistemas.
b) Detección y reacción ante incidentes.
c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

Además, se evaluará la eficacia de las acciones formativas llevadas a cabo.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.4.
– Categoría MEDIA: mp.per.4.
– Categoría ALTA: mp.per.4.

5.3 Protección de los equipos [mp.eq].

5.3.1 Puesto de trabajo despejado [mp.eq.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1 | + R1 |

Requisitos.

– [mp.eq.1.1] Los puestos de trabajo permanecerán despejados, sin que exista material distinto del necesario en cada momento.

Refuerzo R1-Almacenamiento del material.

– [mp.eq.1.r1.1] Una vez usado, y siempre que sea factible, el material se almacenará en lugar cerrado.

Aplicación de la medida.

– Categoría BÁSICA: mp.eq.1.
– Categoría MEDIA: mp.eq.1 + R1.
– Categoría ALTA: mp.eq.1 + R1.

5.3.2 Bloqueo de puesto de trabajo [mp.eq.2].

| dimensiones | A | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | aplica | + R1 |

Requisitos.

– [mp.eq.2.1] El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Refuerzo R1-Cierre de sesiones.

– [mp.eq.2.r1.1] Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

Una Guía CCN-STIC concretará la implementación de la configuración de seguridad adaptada a la categorización del sistema o perfil de cumplimiento asociado.

Aplicación de la medida (por autenticidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.eq.2.
– Nivel ALTO: mp.eq.2 + R1.

5.3.3 Protección de dispositivos portátiles [mp.eq.3].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | +R1+R2 |

Requisitos.

Los equipos (ordenadores portátiles, tabletas, etc.) que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.
Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

– [mp.eq.3.1] Se llevará un inventario de dispositivos portátiles junto con una identificación de la persona responsable de cada uno de ellos y un control regular de que está positivamente bajo su control.
– [mp.eq.3.2] Se establecerá un procedimiento operativo de seguridad para informar al servicio de gestión de incidentes de pérdidas o sustracciones.

– [mp.eq.3.3] Cuando un dispositivo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza.

– [mp.eq.3.4] Se evitará, en la medida de lo posible, que el dispositivo portátil contenga claves de acceso remoto a la organización que no sean imprescindibles. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización u otras de naturaleza análoga.

Refuerzo R1– Cifrado del disco.

– [mp.eq.3.r1.1] Se protegerá el dispositivo portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO.

Refuerzo R2– Entornos protegidos.

– [mp.eq.3.r2.1] El uso de dispositivos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado y a salvo de hurtos y miradas indiscretas.

Aplicación de la medida.

– Categoría BÁSICA: mp.eq.3.
– Categoría MEDIA: mp.eq.3.
– Categoría ALTA: mp.eq.3 + R1 + R2.

5.3.4 Otros dispositivos conectados a la red [mp.eq.4].

| dimensiones | C | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | + R1 | + R1 |

Esta medida afecta a todo tipo de dispositivos conectados a la red y que puedan tener en algún momento acceso a la información, tales como:

a) Dispositivos multifunción: impresoras, escáneres, etc.
b) Dispositivos multimedia: proyectores, altavoces inteligentes, etc.
c) Dispositivos internet de las cosas, en inglés *Internet of Things* (*IoT*).
d) Dispositivos de invitados y los personales de los propios empleados, en inglés *Bring Your Own Device* (BYOD).
e) Otros.

Requisitos.

– [mp.eq.4.1] Los dispositivos presentes en el sistema deberán contar con una configuración de seguridad adecuada de manera que se garantice el control del flujo definido de entrada y salida de la información.

– [mp.eq.4.2] Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la funcionalidad necesaria para eliminar información de soportes de información. (Ver [mp.si.5]).

Refuerzo R1-Productos certificados.

– [mp.eq.4.r1.1] Se usarán, cuando sea posible, productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2-Control de dispositivos conectados a la red.

– [mp.eq.4.r2.1] Se dispondrá de soluciones que permitan visualizar los dispositivos presentes en la red, controlar su conexión/desconexión a la misma y verificar su configuración de seguridad.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.eq.4.
– Nivel MEDIO: mp.eq.4 + R1.
– Nivel ALTO: mp.eq.4+ R1.

5.4 Protección de las comunicaciones [mp.com].

5.4.1 Perímetro seguro [mp.com.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

– [mp.com.1.1] Se dispondrá de un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema.
– [mp.com.1.2] Todos los flujos de información a través del perímetro deben estar autorizados previamente.

La Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información determinará los requisitos establecidos en el perímetro que han de cumplir todos los componentes del sistema en función de la categoría.

Aplicación de la medida.

– Categoría BÁSICA: mp.com.1.
– Categoría MEDIA: mp.com.1.
– Categoría ALTA: mp.com.1.

5.4.2 Protección de la confidencialidad [mp.com.2].

| dimensiones | C | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | + R1 | +R1+R2+R3 |

Requisitos.

– [mp.com.2.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

Refuerzo R1-Algoritmos y parámetros autorizados.

– [mp.com.2.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Dispositivos hardware.

– [mp.com.2.r2.1] Se emplearán, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R3-Productos certificados.

– [mp.com.2.r3.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R4-Cifradores.

– [mp.com.2.r4.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Refuerzo R5-Cifrado de información especialmente sensible.

– [mp.com.2.r5.1] Se cifrará toda la información transmitida.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.com.2.

– Nivel MEDIO: mp.com.2 + R1.
– Nivel ALTO: mp.com.2 + R1 + R2+ R3.

5.4.3 Protección de la integridad y de la autenticidad [mp.com.3].

| dimensiones | I A | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | + R1 + R2 | + R1 + R2 + R3 + R4 |

Requisitos.

– [mp.com.3.1] En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información. (Ver [op.acc.5]).
– [mp.com.3.2] Se prevendrán ataques activos garantizando que al ser detectados se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:

a) La alteración de la información en tránsito.
b) La inyección de información espuria.
c) El secuestro de la sesión por una tercera parte.

– [mp.com.3.3] Se aceptará cualquier mecanismo de identificación y autenticación de los previstos en el ordenamiento jurídico y en la normativa de aplicación.

Refuerzo R1-Redes privadas virtuales.

– [mp.com.3.r1.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

Refuerzo R2-Algoritmos y parámetros autorizados.

– [mp.com.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R3-Dispositivos hardware.

– [mp.com.3.r3.1] Se recomienda emplear dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R4-Productos certificados.

– [mp.com.3.r4.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R5-Cifradores.

– [mp.com.3.r5.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida (por integridad y autenticidad).

– Nivel BAJO: mp.com.3.
– Nivel MEDIO: mp.com.3 + R1 + R2.
– Nivel ALTO: mp.com.3 + R1 + R2 + R3 + R4.

5.4.4 Separación de flujos de información en la red [mp.com.4].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | n.a. | +[R1oR2oR3] | +[R2oR3]+R4 |

La segmentación acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.
Cuando la transmisión de información por la red se restringe a ciertos segmentos, se acota el acceso a la información y los incidentes de seguridad quedan encapsulados en su segmento.

Requisitos.

Los flujos de información se separarán en segmentos de forma que:

– [mp.com.4.1] El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita.
– [mp.com.4.2] Si se emplean comunicaciones inalámbricas, será en un segmento separado.

Refuerzo R1-Segmentación lógica básica.

– [mp.com.4.r1.1] Los segmentos de red se implementarán por medio de redes de área local virtuales (*Virtual Local Area Network, VLAN*).
– [mp.com.4.r1.2] La red que conforma el sistema deberá segregarse en distintas subredes contemplando como mínimo:

• Usuarios.
• Servicios.
• Administración.

Refuerzo R2-Segmentación lógica avanzada.

– [mp.com.4.r2.1] Los segmentos de red se implementarán por medio de redes privadas virtuales (*Virtual Private Network, VPN*).

Refuerzo R3-Segmentación física.

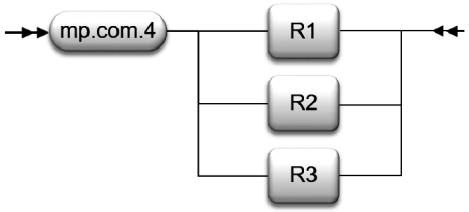
– [mp.com.4.r3.1] Los segmentos de red se implementarán con medios físicos separados.

Refuerzo R4-Puntos de interconexión.

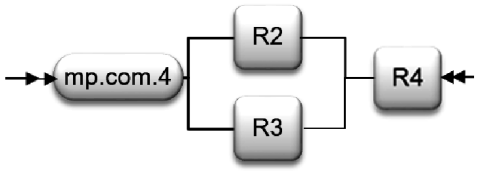
– [mp.com.4.r4.1] Control de entrada de los usuarios que llegan a cada segmento y control de entrada y salida de la información disponible en cada segmento.
– [mp.com.4.r4.2] El punto de interconexión estará particularmente asegurado, mantenido y monitorizado, (como en [mp.com.1]).

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.com.4+ [R1o R2 o R3].




– Categoría ALTA: mp.com.4+[R2 o R3] + R4.




5.5 Protección de los soportes de información [mp.si].

5.5.1 Marcado de soportes [mp.si.1].

| dimensiones | C | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | aplica | aplica |

Requisitos.

– [mp.si.1.1] Los soportes de información (papel impreso, documentos electrónicos, contenidos multimedia -vídeos, cursos, presentaciones- etc.) que contengan información que según [mp.info.2] deba protegerse con medidas de seguridad específicas, llevarán las marcas o metadatos correspondientes que indiquen el nivel de seguridad de la información contenida de mayor calificación.

Refuerzo R1-Marca de agua digital.

– [mp.si.1.r1.1] La política de seguridad de la organización definirá marcas de agua para asegurar el uso adecuado de la información que se maneja.
– [mp.si.1.r1.2] Los soportes de información digital (documentos electrónicos, material multimedia, etc.) podrán incluir una marca de agua según la política de seguridad.
– [mp.si.1.r1.3] Los equipos o dispositivos a través de los que se accede a aplicaciones, escritorios remotos o virtuales, datos, etc., presentarán una marca de agua en pantalla según la política de seguridad.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.si.1.
– Nivel ALTO: mp.si.1.

5.5.2 Criptografía [mp.si.2].

| dimensiones | C I | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | aplica | + R1 + R2 |

Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, *pendrives*, memorias USB u otros de naturaleza análoga.

Requisitos.

– [mp.si.2.1] Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.
– [mp.si.2.2] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R1– Productos certificados.

– [mp.si.2.r1.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R2-Copias de seguridad.

– [mp.si.2.r2.1] Las copias se seguridad se cifrarán utilizando algoritmos y parámetros autorizados por el CCN.

Aplicación de la medida (por confidencialidad e integridad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.si.2.
– Nivel ALTO: mp.si.2 + R1 + R2.

5.5.3 Custodia [mp.si.3].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |

| | | | |
|---|---|---|---|
| | aplica | aplica | aplica |

Requisitos.

– [mp.si.3.1] Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) o lógicas ([mp.si.2]).
– [mp.si.3.2] Se respetarán las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agentes medioambientales.

Aplicación de la medida.

– Categoría BÁSICA: mp.si.3.
– Categoría MEDIA: mp.si.3.
– Categoría ALTA: mp.si.3.

5.5.4 Transporte [mp.si.4].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

El responsable del sistema garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro, fuera de las zonas controladas por la organización.

Requisitos.

– [mp.si.4.1] Se dispondrá de un registro de entrada/salida que identifique al transportista que entrega/recibe el soporte.
– [mp.si.4.2] Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.
– [mp.si.4.3] Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al mayor nivel de seguridad de la información contenida.
– [mp.si.4.4] Se gestionarán las claves según [op.exp.10].

Aplicación de la medida.

– Categoría BÁSICA: mp.si.4.
– Categoría MEDIA: mp.si.4.
– Categoría ALTA: mp.si.4.

5.5.5 Borrado y destrucción [mp.si.5].

| dimensiones | C | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | + R1 | + R1 |

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos y soportes susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Requisitos.

– [mp.si.5.1] Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto del borrado seguro de su contenido que no permita su recuperación. Cuando la naturaleza del soporte no permita un borrado seguro, el soporte no podrá ser reutilizado en ningún otro sistema.

Las guías CCN-STIC del CCN precisarán los criterios para definir como seguro un mecanismo de borrado o de destrucción, en función de la sensibilidad de la información almacenada en el dispositivo.

Refuerzo R1-Productos certificados.

– [mp.si.5.r1.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2 - Destrucción de soportes.

– [mp.si.5.r2.1] Una vez finalizado el ciclo de vida del soporte de información, deberá ser destruido de forma segura conforme a los criterios establecidos por el CCN.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.si.5.
– Nivel MEDIO: mp.si.5 + R1.
– Nivel ALTO: mp.si.5 + R1.

5.6 Protección de las aplicaciones informáticas [mp.sw].

5.6.1 Desarrollo de aplicaciones [mp.sw.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | n.a. | +R1+R2+R3+R4 | +R1+R2+R3+R4 |

Requisitos.

– [mp.sw.1.1] El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción, ni datos de producción en el de desarrollo.

Refuerzo R1-Mínimo privilegio.

– [mp.sw.1.r1.1] Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.

Refuerzo R2-Metodología de desarrollo seguro.

– [mp.sw.1.r2.1] Se aplicará una metodología de desarrollo seguro reconocida que:

a) Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
b) Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (*overflow*).
c) Tratará específicamente los datos usados en pruebas.
d) Permitirá la inspección del código fuente.

Refuerzo R3-Seguridad desde el diseño.

– [mp.sw.1.r3.1] Los siguientes elementos serán parte integral del diseño del sistema:

a) Los mecanismos de identificación y autenticación.
b) Los mecanismos de protección de la información tratada.
c) La generación y tratamiento de pistas de auditoría.

Refuerzo R4-Datos de pruebas.

– [mp.sw.1.r4.1] Preferiblemente, las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales se garantizará el nivel de seguridad correspondiente.

Refuerzo R5-Lista de componentes software.

– [mp.sw.1.r5.1] El desarrollador elaborará y mantendrá actualizada una relación formal de los componentes software de terceros empleados en la aplicación o producto. Se mantendrá un histórico de los componentes utilizados en las diferentes versiones del software. El contenido mínimo de la lista de componentes, que contendrá, al menos, la identificación del componente, el fabricante y la versión empleada, se concretará en una guía CCN-STIC del CCN.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.sw.1 + R1 + R2 + R3 + R4.
– Categoría ALTA: mp.sw.1 + R1 + R2 + R3 + R4.

5.6.2 Aceptación y puesta en servicio [mp.sw.2].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | + R1 | + R1 |

Requisitos.

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

– [mp.sw.2.1] Se comprobará que:

a) Se cumplen los criterios de aceptación en materia de seguridad.
b) No se deteriora la seguridad de otros componentes del servicio.

Refuerzo R1- Pruebas.

– [mp.sw.2.r1.1] Las pruebas se realizarán en un entorno aislado (pre-producción).

Refuerzo R2-Inspección de código fuente.

– [mp.sw.2.r2.1] Se realizará una auditoría de código fuente.

Aplicación de la medida.

– Categoría BÁSICA: mp.sw.2.
– Categoría MEDIA: mp.sw.2 + R1.
– Categoría ALTA: mp.sw.2 + R1.

5.7 Protección de la información [mp.info].

5.7.1 Datos personales [mp.info.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

– [mp.info.1.1] Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

Aplicación de la medida.

– Categoría BÁSICA: mp.info.1.
– Categoría MEDIA: mp.info.1.
– Categoría ALTA: mp.info.1.

5.7.2 Calificación de la información [mp.info.2].

| dimensiones | C | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | aplica | aplica |

Requisitos.

– [mp.info.2.1] Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
– [mp.info.2.2] La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
– [mp.info.2.3] La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I.
– [mp.info.2.4] El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
– [mp.info.2.5] El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.info.2.
– Nivel ALTO: mp.info.2.

5.7.3 Firma electrónica [mp.info.3].

| dimensiones | I A | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | +R1+R2+R3 | + R1+R2+R3+R4 |

Requisitos.

– [mp.info.3.1] Se empleará cualquier tipo de firma electrónica de los previstos en el vigente ordenamiento jurídico, entre ellos, los sistemas de código seguro de verificación vinculados a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre.

Refuerzo R1-Certificados cualificados.

– [mp.info.3.r1.1] Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

Refuerzo R2-Algoritmos y parámetros autorizados.

– [mp.info.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo que resulte de aplicación.

El CCN determinará los algoritmos criptográficos que hayan sido autorizados nominalmente para su uso en el Esquema Nacional de Seguridad conforme a la Instrucción Técnica de Seguridad Criptología de empleo en el ENS.

Refuerzo R3-Verificación y validación de firma.

– [mp.info.3.r3.1] Cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

Refuerzo R4-Firma electrónica avanzada basada en certificados cualificados.

– [mp.info.3.r4.1] Se usará firma electrónica avanzada basada en certificados cualificados complementada por un segundo factor del tipo «algo que se sabe» o «algo que se es».

Refuerzo R5-Firma electrónica cualificada.

– [mp.info.3.r5.1] Se usará firma electrónica cualificada, empleando productos certificados conforme a lo establecido en [op.pl.5].

Aplicación de la medida (por integridad y autenticidad).

– Nivel BAJO: mp.info.3.
– Nivel MEDIO: mp.info.3 + R1 + R2 + R3.
– Nivel ALTO: mp.info.3 + R1 + R2 + R3 + R4.

5.7.4 Sellos de tiempo [mp.info.4].

| dimensiones | T | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | n.a. | aplica |

Requisitos.

La utilización de sellos de tiempo exigirá adoptar las siguientes cautelas:

– [mp.info.4.1] Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
– [mp.info.4.2] Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
– [mp.info.4.3] Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte, en su caso.
– [mp.info.4.4] Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) n.º 910/2014 y normativa de desarrollo.

Refuerzo R1-Productos certificados.

– [mp.info.4.r1.1.] Se utilizarán productos certificados según [op.pl.5].
– [mp.info.4.r1.2] Se asignará una fecha y hora a un documento electrónico, conforme a lo establecido en la guía CCN-STIC Criptología de empleo en el ENS.

Aplicación de la medida (por trazabilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: mp.info.4.

5.7.5 Limpieza de documentos [mp.info.5].

| dimensiones | C | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | aplica | aplica |

Requisitos.

– [mp.info.5.1] En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.info.5.
– Nivel MEDIO: mp.info.5.
– Nivel ALTO: mp.info.5.

5.7.6 Copias de seguridad [mp.info.6].

| dimensiones | D | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | aplica | + R1 | + R1 + R2 |

Requisitos.

– [mp.info.6.1] Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad.
– [mp.info.6.2] Los procedimientos de respaldo establecidos indicarán:

a) Frecuencia de las copias.
b) Requisitos de almacenamiento en el propio lugar.
c) Requisitos de almacenamiento en otros lugares.
d) Controles para el acceso autorizado a las copias de respaldo.

Refuerzo R1-Pruebas de recuperación.

– [mp.info.6.r1.1] Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.

Refuerzo R2-Protección de las copias de seguridad.

– [mp.info.6.r2.1] Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.
– Nivel BAJO: mp.info.6.
– Nivel MEDIO: mp.info.6+ R1.
– Nivel ALTO: mp.info.6+ R1 + R2.

5.8 Protección de los servicios [mp.s].

5.8.1 Protección del correo electrónico [mp.s.1].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | aplica |

Requisitos.

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

– [mp.s.1.1] La información distribuida por medio de correo electrónico se protegerá, tanto en el cuerpo de los mensajes como en los anexos.
– [mp.s.1.2] Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

– [mp.s.1.3] Correo no solicitado, en su expresión inglesa «*spam*».
– [mp.s.1.4] Código dañino, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
– [mp.s.1.5] Código móvil de tipo micro-aplicación, en su expresión inglesa «*applet*».

Se establecerán normas de uso del correo electrónico para el personal. (Ver [org.2]). Estas normas de uso contendrán:

– [mp.s.1.6] Limitaciones al uso como soporte de comunicaciones privadas.
– [mp.s.1.7] Actividades de concienciación y formación relativas al uso del correo electrónico.

Aplicación de la medida.

– Categoría BÁSICA: mp.s.1.
– Categoría MEDIA: mp.s.1.
– Categoría ALTA: mp.s.1.

5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | +[R1oR2] | +[R1oR2] | +R2+R3 |

Requisitos.

Los sistemas que prestan servicios *web* deberán ser protegidos frente a las siguientes amenazas:

– [mp.s.2.1] Cuando la información requiera control de acceso se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular, tomando medidas en los siguientes aspectos:

a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
b) Se prevendrán ataques de manipulación del localizador uniforme de recursos (*Uniform Resource Locator, URL*).
c) Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como *cookies*.
d) Se prevendrán ataques de inyección de código.

– [mp.s.2.2] Se prevendrán intentos de escalado de privilegios.
– [mp.s.2.3] Se prevendrán ataques *de cross site scripting*.

Refuerzo R1-Auditorías de seguridad.

– [mp.s.2.r1.1] Se realizarán auditorías continuas de seguridad de «caja negra» sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción.
– [mp.s.2.r1.2] La frecuencia de estas auditorías de seguridad quedará definida en el procedimiento de auditoría.

Refuerzo R2-Auditorías de seguridad avanzada.

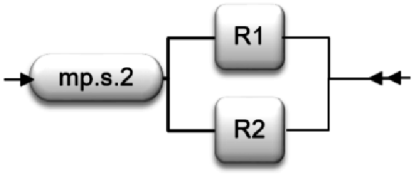
– [mp.s.2.r2.1] Se realizarán auditorías de seguridad de «caja blanca» sobre las aplicaciones web durante la fase de desarrollo.
– [mp.s.2.r2.2] Se emplearán metodologías definidas y herramientas automáticas de detección de vulnerabilidades en la realización de las auditorías de seguridad sobre las aplicaciones web.
– [mp.s.2.r2.3] Una vez finalizada una auditoría de seguridad, se analizarán los resultados y se solventarán las vulnerabilidades encontradas mediante los procedimientos definidos [op.exp.5].

Refuerzo R3-Protección de las cachés.

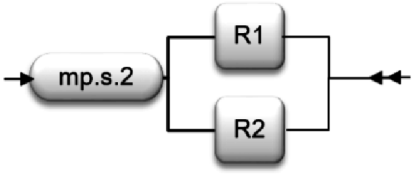
– [mp.s.2.r3.1] Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "*proxies*" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "*cachés*".

Aplicación de la medida.

– Categoría BÁSICA: mp.s.2 + [R1 o R2].




– Categoría MEDIA: mp.s.2 + [R1 o R2].




– Categoría ALTA: mp.s.2 + R2 + R3.

5.8.3 Protección de la navegación web [mp.s.3].

| dimensiones | Todas | | |
|---|---|---|---|
| categoría | BÁSICA | MEDIA | ALTA |
| | aplica | aplica | + R1 |

Requisitos.

El acceso de los usuarios internos a la navegación por internet se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

– [mp.s.3.1] Se establecerá una normativa de utilización, definiendo el uso que se autoriza y las limitaciones de uso personal. En particular, se concretará el uso permitido de conexiones cifradas.
– [mp.s.3.2] Se llevarán a cabo regularmente actividades de concienciación sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos.
– [mp.s.3.3] Se formará al personal encargado de la administración del sistema en monitorización del servicio y respuesta a incidentes.
– [mp.s.3.4] Se protegerá la información de resolución de direcciones web y de establecimiento de conexiones.
– [mp.s.3.5] Se protegerá a la organización en general y al puesto de trabajo en particular frente a problemas que se materializan vía navegación web.
– [mp.s.3.6] Se protegerá contra la actuación de programas dañinos tales como páginas activas, descargas de código ejecutable, etc., previniendo la exposición del sistema a vectores de ataque del tipo *spyware*, *ransomware*, etc.
– [mp.s.3.7] Se establecerá una política ejecutiva de control de cookies, en particular, para evitar la contaminación entre uso personal y uso organizativo.

Refuerzo R1 - Monitorización.

– [mp.s.3.r1.1] Se registrará el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos.
– [mp.s.3.r1.2] Se establecerá una función para la ruptura de canales cifrados a fin de inspeccionar su contenido, indicando qué se analiza, qué se registra, durante cuánto tiempo se retienen los registros y qué uso prevé hacer el organismo de estas inspecciones. Todo

ello sin perjuicio de que se puedan autorizar accesos cifrados singulares a destinos de confianza.

– [mp.s.3.r1.3] Se establecerá una lista negra de destinos vetados.

Refuerzo R2-Destinos autorizados.

– [mp.s.3.r2.1] Se establecerá una lista blanca de destinos accesibles. Todo acceso fuera de los lugares señalados en la lista blanca estará vetado, salvo autorización singular expresa.

Aplicación de la medida.

– Categoría BÁSICA: mp.s.3.
– Categoría MEDIA: mp.s.3.
– Categoría ALTA: mp.s.3 + R1.

5.8.4 Protección frente a la denegación de servicio [mp.s.4].

| dimensiones | D | | |
|---|---|---|---|
| nivel | BAJO | MEDIO | ALTO |
| | n.a. | aplica | + R1 |

Requisitos.

Se establecerán medidas preventivas frente a ataques de denegación de servicio y denegación de servicio distribuido (*Denial of Service, DoS y Distributed Denial of Service, DDoS*). Para ello:

– [mp.s 4.1] Se planificará y dotará al sistema de capacidad suficiente para atender con holgura a la carga prevista.
– [mp.s.4.2] Se desplegarán tecnologías para prevenir los ataques conocidos.

Refuerzo R1-Detección y reacción.

– [mp.s.4.r1.1] Se establecerá un sistema de detección y tratamiento de ataques de denegación de servicio (DoS y DDoS).
– [mp.s. 4.r1.2] Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

Refuerzo R2-Ataques propios.

– [mp.s.4.r2.1] Se detectará y se evitará el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.s.4.
– Nivel ALTO: mp.s.4+ R1.

*6. Valoración de la implantación de las medidas de seguridad*

Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez de capacidad (*Capability Maturity Model, CMM)* permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.

Un proceso es una colección de actividades o tareas relacionadas y estructuradas que, en una secuencia específica, proporciona un servicio para la organización.

Para la valoración de la implantación de las medidas de seguridad, estás se analizarán como procesos y se estimará su nivel de madurez usando el modelo de madurez de capacidad (CMM).

Se identifican cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez:

a) L0-Inexistente.

No existe un proceso que soporte el servicio requerido.

b) L1 - Inicial. Ad hoc.

Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes.

Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.

c) L2-Reproducible, pero intuitivo.

En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad.

Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

d) L3-Proceso definido.

Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.

e) L4-Gestionado y medible.

Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.

f) L5 - Optimizado.

La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Para cada medida de seguridad que sea de aplicación al sistema de información se exigirá un determinado nivel de madurez. Los niveles mínimos de madurez requeridos por el ENS en función de la categoría del sistema son:

| Categoría del sistema | Nivel mínimo de madurez requerido |
|---|---|
| BÁSICA | L2-Reproducible, pero intuitivo. |
| MEDIA | L3-Proceso definido. |
| ALTA | L4-Gestionado y medible. |

*7. Desarrollo y complemento de las medidas de seguridad*

Las medidas de seguridad se desarrollarán y complementarán según lo establecido en la disposición final segunda.

*8. Interpretación*

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en las instrucciones técnicas de seguridad y en las guías CCN-STIC que sean de aplicación a la implementación y a los diversos escenarios de aplicación tales como sedes electrónicas, servicios de validación de certificados electrónicos, servicios de fechado electrónico y validación de documentos fechados, atendiendo el espíritu y finalidad de aquellas.

## ANEXO III

## Auditoría de la seguridad

*1. Objeto de la auditoría*

1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos, al objeto de constatar:

a) Que la política de seguridad define los roles y funciones de los responsables del sistema, la información, los servicios y la seguridad del sistema de información.
b) Que existen procedimientos para resolución de conflictos entre dichos responsables.
c) Que se han designado personas para dichos roles a la luz del principio de «diferenciación de responsabilidades».
d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección, tomando como base la Declaración de Aplicabilidad regulada en el artículo 28 de este real decreto.

1.2 La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los siguientes puntos:

a) Documentación de los procedimientos.
b) Registro de incidentes.
c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
d) Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en artículo 19 «Adquisición de productos de seguridad y contratación de servicios de seguridad».

1.3 Se dispondrá de un programa o plan de auditorías documentado. Las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deberán ser planificadas y acordadas previamente.

*2. Niveles de auditoría*

Los niveles de auditoría que se realizan a los sistemas de información serán los siguientes:

2.1 Auditoría a sistemas de categoría BÁSICA.

a) Los sistemas de información de categoría BÁSICA no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información o en quien éste delegue.
El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular, así como las evidencias que sustentan la valoración anterior.
b) Los informes de autoevaluación serán analizados por el responsable de la seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

2.2 Auditoría a sistemas de categoría MEDIA O ALTA.

a) El informe de auditoría dictaminará sobre el grado de cumplimiento de este real decreto e identificando los hallazgos de conformidad y no conformidad. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.
b) Los informes de auditoría serán analizados por el responsable de la seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

*3. Interpretación*

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los sistemas de información y en la guía CCN-STIC que sea de aplicación, atendiendo al espíritu y finalidad de aquellas.

**ANEXO IV**

**Glosario**

– Activo: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

– Administrador del sistema/de la seguridad del sistema: persona encargada de la instalación y el mantenimiento de un sistema de información, implantando los procedimientos y la configuración de seguridad que se haya establecido en el marco de la política de seguridad del organismo.

– Análisis de riesgos: estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra.

– Área controlada: zona o área en la que una organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella.

– Arquitectura de seguridad: conjunto de elementos físicos y lógicos que forman parte de la arquitectura del sistema y cuyo objetivo es la protección de los activos dentro del sistema y en las interconexiones con otros sistemas.

– Auditoría de la seguridad: es un proceso sistemático, independiente y documentado que persigue la obtención de evidencias objetivas y su evaluación objetiva para determinar en qué medida se cumplen los criterios de auditoría en relación con la idoneidad de los controles de seguridad adoptados, el cumplimiento de la política de seguridad, las normas y los procedimientos operativos establecidos, y detectando desviaciones a los antedichos criterios.

– Autenticación: ratificación de la identidad de un usuario, proceso o dispositivo.

– Autenticación multifactor: exigencia de dos o más factores de autenticación para ratificar una autenticación como válida.

– Autenticador: algo, físico o inmaterial, que posee el usuario bajo su exclusivo control y que le distingue de otros usuarios.

– Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Biometría (factor de autenticación): reconocimiento de los individuos en base a sus características biológicas o de comportamiento.

– Cadena de suministro: conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende a través de la entrega de productos o servicios al usuario final a través de los modos de transporte. Incluye a los proveedores (primer, segundo y tercer nivel), los almacenes de materia prima (directa o indirecta), las líneas de producción, los almacenes de productos terminados y los canales de distribución (mayoristas y minoristas), hasta llegar al cliente final.

– Categoría de seguridad de un sistema: es un grado, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de información a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

– Certificado de firma electrónica (factor de autenticación): una declaración electrónica que vincula los datos de validación de una firma con una persona física o jurídica y confirma, al menos, el nombre o el seudónimo de esa persona.

– Certificado cualificado de firma electrónica: un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

– Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.

– Ciberataque: cualquier conducta dolosa de individuos u organizaciones, conocidos o no, desarrollada a través del ciberespacio contra sistemas de información, con el propósito de sustraer, alterar, abusar, desestabilizar, inutilizar, destruir o eliminar activos.

– Ciberespacio: dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configura un ámbito virtual.

– Ciberincidente: Incidente relacionado con la seguridad de las tecnologías de la información y las comunicaciones que se produce en el ciberespacio.

– Ciberseguridad (seguridad de los sistemas de información): la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

– Compromiso de la seguridad: incidente de seguridad en el que, debido a una violación de las medidas técnicas u organizativas de seguridad, una información o un servicio quedan expuestos, o potencialmente expuestos, a un acceso no autorizado.

– Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

– Contraseña: un secreto memorizado por el usuario, compuesto por varios caracteres según unas reglas de complejidad frente a ataques de adivinación o fuerza bruta.

– Contraseña de un solo uso (*OTP - One-Time Password*): contraseña generada dinámicamente y que solamente se puede usar una vez y durante un periodo limitado.

– Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

– Dispositivo de autenticación (*token*): autenticador físico.

– Distintivo de Certificación de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado electrónicamente por la Entidad de Certificación responsable de la evaluación de los sistemas de información concernidos, incluyendo un enlace a la Certificación de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate.

– Distintivo de Declaración de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado o sellado electrónicamente por la entidad bajo cuya responsabilidad se encuentre el sistema de información en cuestión, incluyendo un enlace a la Declaración de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada de que se trate.

– Dominio de seguridad: colección de activos uniformemente protegidos, típicamente bajo una única autoridad. Los dominios de seguridad se utilizan para diferenciar entre zonas en el sistema de información. Por ejemplo:

a) Instalaciones centrales, sucursales, comerciales trabajando con portátiles.
b) Servidor central (host), frontal Unix y equipos administrativos.
c) Seguridad física, seguridad lógica.

– Evento de seguridad: ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, una falla de los controles o una situación desconocida que puede ser relevante para la seguridad.

– Factor de autenticación: hay 3 tipos de factores de autenticación: (1) algo que se sabe, un secreto; (2) algo que se tiene, un autenticador; y (3) algo que se es, biometría.

– Firma electrónica: los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

– Firma electrónica avanzada: la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

– Firma electrónica cualificada: una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

– Gestión de incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

– Gestión de riesgos: actividades coordinadas para dirigir y controlar a una organización con respecto a los riesgos.

– Incidente de seguridad (ciberincidente o incidente): suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

– Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

– Lista de componentes software: documento que detalla los componentes software utilizados para construir algo, sea una aplicación o un servicio.

– Medidas de seguridad: conjunto de disposiciones encaminadas a proteger al sistema de información de los riesgos a los que estuviere sometido, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

– Mínimo privilegio: principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento.

– Monitorización continua: proceso de gestión dinámica de la seguridad basado en el seguimiento de indicadores críticos de seguridad y parcheo de las vulnerabilidades descubiertas en los componentes del sistema de información.

– Observatorio Digital: un observatorio digital, en su propósito de conocer realidades de la información que se transmite a través de medios digitales, es un conjunto de capacidades para la toma de decisiones dedicado a la detección y seguimiento de anomalías en el origen, definición o diseminación de contenidos digitales, las cuales pudieran representar indicadores de amenaza.

– Perfil de cumplimiento específico: conjunto de medidas de seguridad, comprendidas o no en el anexo II de este real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN.

– PIN: un secreto memorizado por el usuario, compuesto por unos pocos caracteres, siguiendo unas ciertas reglas frente a ataques de adivinación.

– Política de firma electrónica, sello electrónico y certificados: conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas y sellos electrónicos, incluyendo las características exigibles a los certificados de firma o sello electrónicos.

– Política de seguridad (Política de seguridad de la información): conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.

– Principios básicos de seguridad: fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

– Proceso: conjunto organizado de actividades que se llevan a cabo para producir un producto o prestar un servicio, que tiene un principio y fin delimitados, que implica recursos y da lugar a un resultado.

– Proceso de seguridad: método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

– Proceso TIC: conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio TIC.

– Producto TIC: elemento o grupo de elementos de las redes o los sistemas de información.

– Requisitos mínimos de seguridad: exigencias mínimas necesarias para asegurar la información tratada y los servicios prestados.

– Secreto memorizado (factor de autenticación): algo que solamente sabe el usuario autorizado. Típicamente, se concreta en una contraseña o un PIN.

– Sistema de información: cualquiera de los elementos siguientes:

1.º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.

2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.

3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

– TEMPEST: término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.

– Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.

– USO OFICIAL: designa información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.

– Usuarios de la organización: personal del organismo, propio o contratado, estable o circunstancial, que acceden al sistema para desarrollar las funciones o actividades que les han sido encomendadas por la organización.

– Usuarios externos: usuarios con acceso al sistema que no entran en el conjunto de usuarios de la organización. En particular, los ciudadanos administrados.

# § 26

## Resolución de 7 de julio de 2021, de la Secretaría General de Administración Digital, por la que se aprueba la Política de Seguridad de los servicios prestados por la Secretaría General de Administración Digital

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 172, de 20 de julio de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-12148

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas regula en su artículo 13 los derechos de las personas en sus relaciones con las Administraciones Públicas, incluyendo en su apartado h) el relativo a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, al regular en su artículo 3 los principios generales que las Administraciones Públicas deben respetar en su actuación y relaciones, establece en su apartado 2 que aquellas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

En el artículo 156.2 de la misma norma prevé la existencia del Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

El Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica se regula en el Real Decreto 3/2010, de 8 de enero, cuyo artículo 11.1 establece el mandato de que todos los órganos superiores de las Administraciones públicas dispongan formalmente de su política de seguridad aprobada por su titular, que articule la gestión continuada de la seguridad. Dicha política de seguridad se establecerá de acuerdo con los principios básicos que recogen los artículos 4 a 10 y se desarrollará aplicando los requisitos mínimos que detalla el propio artículo 11.1.

El anexo II del real decreto, al regular las medidas de seguridad, incluye el marco organizativo entre el primer grupo de dichas medidas, que comprende, entre otras, la política de seguridad. Al respecto, el apartado 3.1 del Anexo II establece que la política de seguridad debe referenciar y ser coherente con lo establecido en la legislación de protección de datos de carácter personal, en lo que corresponda, en particular, por el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo

que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y por lo previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital en el artículo 9 atribuye a la Secretaría General de Administración Digital (en adelante, SGAD), un amplio conjunto de competencias de carácter transversal a toda la Administración General del Estado y sus Organismos Públicos, entre ellas la provisión de servicios en materia de tecnologías de la información y comunicaciones y la prestación de aplicaciones y servicios para Delegaciones y Subdelegaciones del Gobierno y las Direcciones Insulares en todos sus ámbitos de actuación, en materia de tecnologías de la información y comunicaciones.

A la luz de las competencias previstas en el artículo 9 del Real Decreto 403/2020, de 25 de febrero, y en coherencia con la estrategia de racionalización encomendada a la Secretaría General de Administración Digital, la presente resolución tiene como finalidad aprobar la Política de Seguridad única en el ámbito de todos los servicios de tecnologías de la información prestados por la Secretaría General de Administración Digital, independientemente de la adscripción orgánica de la Unidad destinataria de los mismos. Asimismo, la resolución establece la estructura organizativa necesaria para desarrollar, implantar y gestionar esta política.

En virtud de lo anterior, en cumplimiento del artículo 11 del Real Decreto 3/2010, de 8 de enero, previo informe de la Abogacía del Estado, dispongo:

**Primero.**

Se aprueba la «Política de Seguridad de los servicios prestados por la Secretaría General de Administración Digital», cuyo texto se incluye a continuación.

**Segundo.**

La Política de seguridad de los servicios prestados por la Secretaría General de Administración Digital se aplicará desde el día siguiente al de la publicación de la presente Resolución en el «Boletín Oficial del Estado».

## POLÍTICA DE SEGURIDAD DE LOS SERVICIOS PRESTADOS POR LA SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

**Artículo 1.** *Objeto.*

1. La Política de Seguridad de los servicios prestados por la Secretaría General de Administración Digital (en adelante, SGAD) tiene por objeto identificar responsabilidades y establecer principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por la Secretaría General de Administración Digital mediante las tecnologías de la información y de las comunicaciones, así como la estructuración de la correspondiente documentación de seguridad.

2. La Política de Seguridad es el instrumento en el que se apoya la Secretaría General de Administración Digital para garantizar el uso seguro de los sistemas de información y las comunicaciones, en el ejercicio de las competencias, previstas en el artículo 9 del Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital.

**Artículo 2.** *Misión y funciones de la Secretaría General de Administración Digital.*

Sin perjuicio del resto de competencias previstas en el artículo 9 del Real Decreto 403/2020, de 25 de febrero, las competencias de la Secretaría General de Administración Digital relativas a la prestación de servicios se encuadran en los siguientes ejes de actuación:

a) Prestación de Servicios TIC comunes y de carácter horizontal, incluidos los servicios declarados compartidos por la Comisión de Estrategia TIC en su reunión de 15 de septiembre de 2015, u otros que puedan ser declarados con posterioridad.

b) Prestación de Servicios TIC sectoriales, tanto los prestados por la Secretaría General de Administración Digital en virtud de sus competencias como los prestados a aquellos órganos, unidades, organismos y entes públicos con los que se acuerde la provisión.

c) Prestación de servicios directos a ciudadanos y empresas.

**Artículo 3.** *Principios rectores de la Política de Seguridad.*

Los principios básicos y requisitos de la seguridad de la información desarrollados bajo el marco de esta Política de Seguridad son los recogidos en el Esquema Nacional de Seguridad regulado por el Real Decreto 3/2010, de 8 de enero, en particular, los previstos en sus capítulos II y III, y su normativa de desarrollo.

**Artículo 4.** *Desarrollo normativo.*

1. El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en tres niveles, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: constituido por la presente Política de Seguridad.

b) Segundo nivel normativo: constituido principalmente por las normas y directrices de seguridad generales que, respetando lo estipulado por la Política de Seguridad, determinan qué se puede hacer y qué no desde el punto de vista de la seguridad en relación con los servicios prestados por la Secretaría General de Administración Digital, sin considerar aspectos relativos a implementación ni tecnológicos.

La documentación perteneciente a este segundo nivel normativo será aprobada por Resolución del Secretario General de Administración Digital a propuesta del Responsable de Seguridad, previo acuerdo en el Grupo de Trabajo de Seguridad de los servicios prestados por la Secretaría General de Administración Digital.

c) Tercer nivel normativo: constituido por políticas específicas que, respetando lo dispuesto en los niveles normativos anteriores, apliquen a ámbitos o sistemas de información particulares. También estará constituido por procedimientos, guías e instrucciones de carácter técnico o procedimental.

La documentación perteneciente a este tercer nivel normativo será aprobada por el Responsable de Seguridad, previo acuerdo en el Grupo de Trabajo de Seguridad de los servicios prestados por la Secretaría General de Administración Digital.

2. El Responsable de Seguridad será el encargado de mantener la documentación de seguridad actualizada y organizada, y de gestionar los mecanismos de acceso a la misma.

3. El personal de cada uno de los órganos u organismos a los que es de aplicación la presente Política de Seguridad tendrá la obligación de conocerla y cumplirla y las normas y procedimientos de seguridad de la información que puedan afectar a sus funciones. A tal efecto, la Secretaría General de Administración Digital pondrá a disposición de todas las entidades usuarias de sus servicios la documentación pertinente.

**Artículo 5.** *Estructura organizativa.*

1. La organización de la seguridad tendrá en cuenta la organización propia de la Secretaría General de Administración Digital y la de los órganos, organismos y entidades usuarios de sus servicios. En consecuencia, deberá garantizarse la actuación coordinada y eficaz, según lo establecido al respecto en el Esquema Nacional de Seguridad y en las orientaciones de la guía CCN-STIC 801 ‘Responsabilidades y funciones’.

2. Sin perjuicio de lo anterior, son órganos que intervienen en el desarrollo de la presente Política de Seguridad:

a) El Secretario General de Administración Digital.

b) El Grupo de trabajo de seguridad de los servicios prestados por la Secretaría General de Administración Digital.

c) El Responsable de Seguridad.
d) El Responsable del Sistema.
e) Los Responsables de la Información.
f) Los Responsables del Servicio.
g) Los Delegados de Protección de Datos

3. Los órganos u organismos sujetos a la presente Política de Seguridad deberán disponer de la estructura organizativa necesaria para cumplir adecuadamente con sus obligaciones en el ámbito de los servicios que presta la Secretaría General de Administración Digital.

**Artículo 6.** *Competencias del Secretario General de Administración Digital.*

La persona titular de la Secretaría General de Administración Digital es, en el ejercicio de sus competencias, el responsable del funcionamiento de los servicios que presta la Secretaría General de Administración Digital. En particular:

a) Coordinará todas las actividades relacionadas con la seguridad de los servicios prestados por la Secretaría General de Administración Digital, tanto de carácter horizontal, común o compartido, como de carácter sectorial.
b) Impulsará la adecuación a la normativa aplicable de seguridad de la información y de protección de datos, dentro de su ámbito de competencias.
c) Será responsable de la modificación y actualización de esta Política de Seguridad, así como de aprobar las normas de seguridad propuestas por el Responsable de Seguridad, previo acuerdo del Grupo de Trabajo de seguridad de los servicios prestados por la Secretaría General de Administración Digital.

**Artículo 7.** *Grupo de trabajo de seguridad de los servicios prestados por la Secretaría General de Administración Digital.*

1. Con carácter permanente, se crea el Grupo de trabajo de seguridad de los servicios prestados por la Secretaría General de Administración Digital (en adelante, GTS) como órgano de asesoramiento del Secretario General de Administración Digital en materia de seguridad.
El GTS estará compuesto por:

a) Presidente: el Responsable de Seguridad de la Secretaría General de Administración Digital.
b) Vicepresidente: el Responsable del Sistema de la Secretaría General de Administración Digital.
c) Un vocal de cada una de las siguientes unidades de la Secretaría General de Administración Digital designado por el titular respectivo:

1.º La División de Planificación y Coordinación de Ciberseguridad.
2.º La Subdirección General de Planificación y Gobernanza de la Administración Digital.
3.º La Subdirección General de Impulso de la Digitalización de la Administración.
4.º La Subdirección General de Infraestructuras y Operaciones.
5.º La Subdirección General de Servicios Digitales para la Gestión.
6.º La Subdirección General de Presupuestos y Contratación TIC.
7.º El Gabinete de la Secretaría General de Administración Digital.

d) Secretario: un funcionario de la División de Planificación y Coordinación de Ciberseguridad, nombrado por su titular, que actuará con voz pero sin voto.

2. Cada unidad representada en el GTS podrá convocar a personal en calidad de asesor, con voz, pero sin voto.
3. El Presidente podrá convocar, en razón de los asuntos tratados, a representantes de cualquier órgano y unidad que accedan a sistemas de información de la Secretaría General de Administración Digital, así como a expertos tanto de la Secretaría General de Administración Digital como de otras entidades.
4. El GTS llevará a cabo las siguientes funciones:

a) Elaborar estudios, análisis y propuestas de modificación y actualización de la Política de Seguridad y de la normativa de la seguridad de la información de segundo y tercer nivel.

b) Solicitar al Responsable de Seguridad la toma en consideración de cualquier aspecto que considere relevante respecto a la seguridad de la información.

c) Velar por la coherencia y armonización de la normativa y actuaciones en materia de seguridad de la información entre los distintos servicios ofrecidos por la Secretaría General de Administración Digital, ya sean los de carácter común, horizontal o sectorial.

d) Asesorar al Responsable de Seguridad en la preparación o confección de la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

e) Estudiar y proponer actividades de concienciación y formación en materia de seguridad.

f) Realizar cualquier otra actividad de asesoría, formulación de recomendaciones, o propuesta de iniciativas, en materia de seguridad.

g) Cualquier otra función en el ámbito de la seguridad de la información y los servicios que le encomiende el Secretario General de Administración Digital.

5. El GTS se reunirá al menos una vez al cuatrimestre y sus decisiones se adoptarán por mayoría de sus miembros con derecho a voto.

**Artículo 8.** *Responsable de Seguridad.*

1. El Director de la División de Planificación y Coordinación de Ciberseguridad, en su condición de Responsable de Seguridad en el ámbito de la presente Política de Seguridad, es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, de acuerdo con lo previsto en el artículo 10 del Real Decreto 3/2010, de 8 de enero.

2. El ámbito de actuación del Responsable de Seguridad se extiende a todos los servicios prestados por la Secretaría General de Administración Digital, debiendo velar por la coherencia y armonización de las normas, procedimientos y actuaciones de la Secretaría General de Administración Digital en los diferentes ámbitos.

3. Son funciones específicas del Responsable de Seguridad:

a) Promover la seguridad de los servicios prestados por la Secretaría General de Administración Digital y la mejora continua en su gestión.

b) Proponer al SGAD, previo acuerdo del GTS, la aprobación de la normativa de seguridad de segundo nivel.

c) Aprobar la normativa de seguridad de tercer nivel, previo acuerdo del GTS.

d) Impulsar y velar por el cumplimiento y difusión de la Política de Seguridad y de su cuerpo normativo, promoviendo las actividades de concienciación y formación en materia de seguridad para todo el personal afectado por la Política de Seguridad.

e) Asesorar, en colaboración con el Responsable del Sistema, a los Responsables de la Información y Responsables del Servicio, en la realización de los preceptivos análisis de riesgos.

f) Determinar, junto con el Responsable del Sistema, la agrupación en sistemas de los servicios TIC prestados por la Secretaría General de Administración Digital, y la categoría de estos sistemas, según el procedimiento descrito en el anexo I del Real Decreto 3/2010, de 8 de enero; y determinar las medidas de seguridad que deben aplicarse, de acuerdo con lo previsto en el anexo II del Real Decreto 3/2010, de 8 de enero.

g) Aprobar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

h) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes fruto de las mismas.

i) Proponer las decisiones respecto a medidas de contingencia que considere imprescindibles para preservar la seguridad de los servicios prestados por la Secretaría General de Administración Digital.

j) Informar periódicamente al SGAD sobre el estado de la seguridad en el ámbito de esta Política de Seguridad. Para ello podrá utilizar informes de incidentes de seguridad, resultados de auditorías y análisis de riesgos realizados, y, en general, cualquier información

de seguridad relevante que pueda recabar en el desarrollo de sus funciones, o a través de solicitud al GTS.

k) Realizar cualquier otra actividad relativa a la seguridad de los servicios prestados por la Secretaría General de Administración Digital.

4. El Responsable de Seguridad podrá designar motivadamente, siendo responsable de su actuación, los Responsables de Seguridad Delegados que considere necesarios para el adecuado cumplimiento de sus funciones, quienes actuarán bajo su coordinación y de acuerdo con sus criterios.

**Artículo 9.** *Responsable del Sistema.*

1. El Responsable del Sistema, nombrado por el Secretario General de Administración Digital, tiene la responsabilidad de desarrollar, operar y mantener el sistema de información que soporta los distintos servicios, durante todo su ciclo de vida.

Su ámbito de actuación se extenderá a todos los sistemas que sustentan servicios prestados por la Secretaría General de Administración Digital, con independencia de su naturaleza.

2. Son funciones del Responsable del Sistema:

a) Implantar las medidas necesarias para garantizar la seguridad del servicio durante todo su ciclo de vida, contando con el asesoramiento del Responsable de Seguridad del ámbito de competencia correspondiente.

b) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

c) Asesorar, en colaboración con el Responsable de Seguridad, a los Responsables de la Información y a los Responsables del Servicio en la realización de los preceptivos análisis de riesgos.

d) Determinar, junto con el Responsable de Seguridad, la agrupación de los servicios TIC prestados por la Secretaría General de Administración Digital en sistemas, y la categoría de estos sistemas, según el procedimiento descrito en el anexo I del Real Decreto 3/2010, de 8 de enero.

e) Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado o detecta deficiencias graves de seguridad, previo acuerdo con el Responsable de dicha información o servicio, y con el Responsable de Seguridad.

3. El Responsable del Sistema deberá coordinar las actuaciones de interconexión y acceso a los servicios de la Secretaría General de Administración Digital con los responsables del sistema de los organismos o entidades a los que la Secretaría General de Administración Digital preste sus servicios, bajo las directrices establecidas por el cuerpo normativo de seguridad.

4. El Responsable del Sistema podrá designar motivadamente, siendo responsable de su actuación, los Responsables de Sistema Delegados que considere necesarios para el adecuado cumplimiento de sus funciones, quienes actuarán bajo su coordinación y de acuerdo con sus criterios.

**Artículo 10.** *Responsables de la Información y Responsables del Servicio.*

1. De acuerdo con lo previsto en el artículo 10 del Real Decreto 3/2010, de 8 de enero, y en la correspondiente guía CCN-STIC sobre roles y funciones en el ENS, en los sistemas de información el responsable de la información determinará los requisitos de la información tratada y el responsable del servicio determinará los requisitos de los servicios prestados.

2. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.

3. Dado que la Secretaría General de Administración Digital ofrece servicios a otras entidades, incluidos servicios sectoriales y servicios horizontales, comunes y compartidos a otras entidades, los Responsables de la Información o del Servicio pertenecerán en general a esas otras entidades, que nombrarán a los citados responsables y los comunicarán al SGAD. El modelo de relación con estos representantes lo establecerá la Secretaría General de Administración Digital conforme al modelo de prestación de cada servicio.

4. En caso de que un servicio prestado por un sistema de información de la Secretaría General de Administración Digital se realice en la nube, en modo multicliente, y dicho servicio no tenga Responsables de la Información o del Servicio nombrados, la Secretaría General de Administración Digital podrá asumir las funciones de Responsable de la Información o del Servicio en el ámbito de dicho sistema de información.

5. Los Responsables de la Información o del Servicio asistirán, conforme a lo dispuesto en el artículo 7 de esta Política de Seguridad, a las reuniones del GTS de los servicios prestados por la Secretaría General de Administración Digital, cuando sean requeridos por su Presidente.

6. Las funciones de cada Responsable de Información y Responsable del Servicio, dentro de su ámbito de actuación y con el asesoramiento y colaboración del Responsable de Seguridad y el Responsable del Sistema serán las siguientes:

a) Determinar los niveles de seguridad de la información tratada y de los servicios prestados, respectivamente.

b) Realizar, con el asesoramiento del Responsable de Seguridad y del Responsable del Sistema, los preceptivos análisis de riesgos y auditorías de seguridad, acordando con dichos responsables las salvaguardas a implantar.

c) Aceptar los riesgos residuales calculados en el análisis de riesgos.

**Artículo 11.** *Delegados de Protección de Datos.*

Los Delegados de Protección de Datos desempeñarán, cuando la Secretaría General de Administración Digital sea Encargada del tratamiento, y dentro de su ámbito de actuación y de sus competencias, las funciones del Delegado de Protección de Datos indicadas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de Abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y demás disposiciones reguladoras de la materia.

**Artículo 12.** *Resolución de conflictos.*

En caso de conflicto entre los diferentes responsables, éste será resuelto por su superior jerárquico, si pertenecen al mismo órgano superior. En su defecto resolverá el Secretario General de Administración Digital.

# § 27

## Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 265, de 2 de noviembre de 2016
Última modificación: sin modificaciones
Referencia: BOE-A-2016-10108

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos.

El Real Decreto 3/2010, de 8 de enero, prevé en su artículo 29 apartado 2 que el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento y se publicarán mediante resolución de la Secretaría de Estado de Administraciones Públicas. Dichas instrucciones técnicas de seguridad son esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el Esquema.

Así, estas instrucciones técnicas de seguridad, enumeradas en la Disposición Adicional cuarta del citado Real Decreto, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como: Informe del Estado de la Seguridad; notificación de incidentes de Seguridad; auditoría de la Seguridad; conformidad con el Esquema Nacional de Seguridad; adquisición de Productos de Seguridad; criptología de empleo en el Esquema Nacional de Seguridad; interconexión en el Esquema Nacional de Seguridad y Requisitos de Seguridad en entornos externalizados, sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica, según lo establecido en el citado artículo 29.

Estas instrucciones técnicas de seguridad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

En particular, la Instrucción Técnica de Seguridad de Informe Nacional del Estado de la Seguridad, establece las condiciones relativas a la recopilación y comunicación de datos que permita conocer las principales variables de la seguridad de la información de los sistemas

comprendidos en el ámbito de aplicación del Esquema Nacional de Seguridad, y confeccionar un perfil general del estado de la ciberseguridad en las Administraciones públicas, al objeto de poder dar adecuada respuesta al mandato del artículo 35 del Real Decreto 3/2010, de 8 de enero.

Esta Resolución se aprueba en aplicación de lo dispuesto en el artículo 29 apartado 2 del Real Decreto 3/2010, de 8 de enero, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional. En virtud de lo anterior, esta Secretaría de Estado resuelve:

**Primero.**

Aprobar la Instrucción Técnica de Seguridad «Informe del Estado de la Seguridad», cuyo texto se incluye a continuación.

**Segundo.**

Ordenar su publicación en el «Boletín Oficial del Estado».

**INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE INFORME DEL ESTADO DE LA SEGURIDAD**

I. Objeto: La Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad tiene por objeto establecer las condiciones relativas a la recopilación y comunicación de datos que permita conocer las principales variables de la seguridad de la información de los sistemas comprendidos en el ámbito de aplicación del Esquema Nacional de Seguridad, y confeccionar un perfil general del estado de la ciberseguridad en las Administraciones públicas.

II. Ámbito de aplicación: La presente Instrucción Técnica de Seguridad será de aplicación a los sistemas de información comprendidos en lo dispuesto en el artículo 3 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

III. Recopilación y comunicación de datos:

III.1 Las entidades públicas comprendidas en el ámbito de aplicación de la presente Instrucción Técnica de Seguridad recopilarán los datos de las diferentes variables de seguridad conforme a lo dispuesto en la medida «sistema de métricas [op.mon.2]» del Anexo II del Real Decreto 3/2010, de 8 de enero.

III.2 Las entidades públicas a las que se refiere el punto anterior comunicarán, al menos con carácter anual, el estado de las principales variables de seguridad de aquellos sistemas de información que se encuentren bajo su responsabilidad.

III.3 Para la comunicación a la que se refiere el punto anterior, el Responsable de Seguridad de los sistemas de información afectados de la entidad pública, o en quien este delegue, utilizará la herramienta relativa al Informe Nacional del Estado de la Seguridad (INES), al que tendrá acceso, previa identificación, en el siguiente enlace: https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ines.html

III.4 El Centro Criptológico Nacional, en cumplimiento del artículo 29 apartado 1 del Real Decreto 3/2010, de 8 de enero mantendrá un Manual de Usuario de la herramienta INES, permanentemente actualizado a través de la guía de seguridad CCN-STIC 844.

IV. Tratamiento de datos:

IV.1 Los datos que la herramienta INES requerirá de la entidad pública del ámbito de aplicación de la presente Instrucción Técnica de Seguridad son los que se señalan en la guía de seguridad CCN-STIC 824 Informe del Estado de Seguridad, que el Centro Criptológico Nacional mantendrá permanentemente actualizada y, en general, estarán referidos a identificación de la entidad, datos generales, organización de la seguridad, procesos críticos, concienciación y formación, gestión de incidentes, recursos y presupuestos, auditoría, indicadores críticos de riesgo y medidas de seguridad, según lo descrito en la guía de seguridad CCN-STIC-815 sobre Métricas e Indicadores para el Esquema Nacional de Seguridad.

# § 28

## Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 265, de 2 de noviembre de 2016
Última modificación: sin modificaciones
Referencia: BOE-A-2016-10109

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos.

El Real Decreto 3/2010, de 8 de enero, prevé en su artículo 29 apartado 2 que el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento y se publicarán mediante resolución de la Secretaría de Estado de Administraciones Públicas. Dichas instrucciones técnicas de seguridad son esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el Esquema.

Así, estas instrucciones técnicas de seguridad, enumeradas en la disposición adicional cuarta del citado Real Decreto, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como: Informe del Estado de la Seguridad; notificación de incidentes de Seguridad; auditoría de la Seguridad; conformidad con el Esquema Nacional de Seguridad; adquisición de Productos de Seguridad; criptología de empleo en el Esquema Nacional de Seguridad; interconexión en el Esquema Nacional de Seguridad y Requisitos de Seguridad en entornos externalizados, sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica, según lo establecido en el citado artículo 29.

Estas instrucciones técnicas de seguridad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

En particular, la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad establece los criterios y procedimientos para la determinación de la

conformidad con el Esquema Nacional de Seguridad y para la publicidad de dicha conformidad, al objeto de poder dar adecuada respuesta al mandato del Capítulo VIII, Normas de conformidad, del Real Decreto 3/2010, de 8 de enero; así, determina los mecanismos de obtención y ulterior publicidad de las declaraciones de conformidad y los distintivos de seguridad de los que sean acreedores y que se hubieren obtenido respecto al cumplimiento del Esquema Nacional de Seguridad.

Esta Resolución se aprueba en aplicación de lo dispuesto en el artículo 29 apartado 2 del Real Decreto 3/2010, de 8 de enero, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional. En virtud de lo anterior, esta Secretaría de Estado resuelve:

**Primero.**

Aprobar la Instrucción Técnica de Seguridad «Conformidad con el Esquema Nacional de Seguridad», cuyo texto se incluye a continuación.

**Segundo.**

Ordenar su publicación en el «Boletín Oficial del Estado».

La Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

### *I. Objeto*

La Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad tiene por objeto establecer los procedimientos para dar publicidad a la conformidad con el Esquema Nacional de Seguridad, así como los requisitos exigibles a las entidades certificadoras.

### *II. Ámbito de aplicación*

La presente Instrucción Técnica de Seguridad será de aplicación a los sistemas de información comprendidos en lo dispuesto en el artículo 3 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

### *III. Procedimientos de determinación de la conformidad*

III.1 En función de la categoría de los sistemas de información del ámbito de aplicación del Esquema Nacional de Seguridad, de acuerdo con el Anexo I del Real Decreto 3/2010, de 8 de enero, se define el procedimiento de determinación de la conformidad. Así los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, mientras que los sistemas de categoría MEDIA O ALTA precisarán de una auditoría formal para su certificación de la conformidad.

III.2 La declaración de la conformidad con el Esquema Nacional de Seguridad de los sistemas de información con categoría BÁSICA se realizará mediante una autoevaluación que, con carácter ordinario, verifique el cumplimiento de los requerimientos contemplados en el Esquema, al menos cada dos años. Dicha autoevaluación atenderá a lo dispuesto sobre auditoría en el artículo 34 y en el anexo III del Real Decreto 3/2010, de 8 de enero. Dicha autoevaluación podrá ser desarrollada por el mismo personal que administra el sistema de información o en quién éste delegue.

III.3 La certificación de la conformidad con el Esquema Nacional de Seguridad de los sistemas de información con categorías MEDIA o ALTA se realizará mediante un procedimiento de auditoría formal que, con carácter ordinario, verifique el cumplimiento de

los requerimientos contemplados en el Esquema, al menos cada dos años. Dicha auditoría se realizará según lo dispuesto en el artículo 34 y en el anexo III del Real Decreto 3/2010, de 8 de enero.

III.4 Siendo obligatoria la auditoría formal para los sistemas de categoría MEDIA Y ALTA nada impide que un sistema de categoría BÁSICA se someta igualmente a una auditoria formal de certificación de la conformidad, siendo esta posibilidad siempre la deseable.

III.5 En las comunidades autónomas con lengua cooficial se podrán expedir las declaraciones, certificaciones y sus respectivos distintivos de conformidad en castellano o bien en texto bilingüe. En este caso, se expedirán en un solo documento redactado en castellano y en la correspondiente lengua cooficial, en tipos de letra de igual rango con las especificaciones y diligencias que sobre su texto se establecen en los anexos correspondientes.

*IV. Declaración de Conformidad con el Esquema Nacional de Seguridad de sistemas de categoría BÁSICA y su publicidad*

IV.1 La Declaración de Conformidad con el Esquema Nacional de Seguridad de sistemas de categoría BÁSICA o inferior será expedida por la propia entidad bajo cuya responsabilidad se encuentren dichos sistemas, y se completará mediante un Distintivo de Declaración de Conformidad cuyo uso estará condicionado a la antedicha Declaración de Conformidad.

IV.2 Dicha Declaración de Conformidad así como su distintivo se expresarán en documentos electrónicos, en formato no editable y poseerán el aspecto que se muestra en los Anexos I y II respectivamente de la presente Instrucción Técnica de Seguridad.

IV.3 Para publicar la Declaración de Conformidad con el Esquema Nacional de Seguridad en el caso de sistemas de información de categoría BÁSICA o inferior bastará con la exhibición en la sede electrónica de la entidad pública titular o usuaria del sistema de información en cuestión, del Distintivo de Declaración de Conformidad que incluirá un enlace al documento de Declaración de Conformidad correspondiente, que también permanecerá accesible a través de dicha sede electrónica.

*V. Certificación de Conformidad con el Esquema Nacional de Seguridad de sistemas de categoría MEDIA o ALTA y su publicidad*

V.1 La Certificación de Conformidad con el Esquema Nacional de Seguridad, de sistemas de categorías MEDIA o ALTA, será expedida por una entidad certificadora y se completará mediante un Distintivo de Certificación de Conformidad cuyo uso estará condicionado a la antedicha Certificación de Conformidad.

V.2 Dicha Certificación de Conformidad así como su distintivo se expresarán en documentos electrónicos, en formato no editable y poseerán el aspecto que se muestra en los Anexos III y IV respectivamente de la presente Instrucción Técnica de Seguridad.

V.3 Para publicar la Certificación de Conformidad con el Esquema Nacional de Seguridad en el caso de sistemas de información de categoría MEDIA O ALTA bastará con la exhibición en la sede electrónica de la entidad pública titular o usuaria del sistema de información en cuestión, del Distintivo de Certificación de Conformidad que incluirá un enlace al documento de Certificación de Conformidad correspondiente, que también permanecerá accesible a través de dicha sede electrónica.

*VI. Requisitos de las entidades certificadoras*

VI.1 Las entidades certificadoras a las que se refiere esta Instrucción Técnica deberán estar acreditadas por la Entidad Nacional de Acreditación (ENAC) para la certificación de sistemas del ámbito de aplicación del Esquema Nacional de Seguridad conforme a la norma UNE-EN ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.

VI.2 Si la entidad certificadora de que se trate no dispusiere de la acreditación señalada, previamente a iniciar sus actividades, deberá remitir al Centro Criptológico Nacional, la aceptación por parte de la Entidad Nacional de Acreditación de haber solicitado la

acreditación antedicha, pudiendo iniciar sus actividades de certificación de forma transitoria, disponiendo de 12 meses para obtener dicha acreditación, transcurridos los cuales sin haberla obtenido deberán cesar en sus actividades de certificación. El Centro Criptológico Nacional podrá requerir a la entidad certificadora solicitante cuanta información adicional considere necesaria que le permita verificar su adecuación y suficiencia.

VI.3 Transcurrido un año desde la entrada en vigor de la presente Instrucción Técnica de Seguridad, ya no será posible iniciar ningún proceso de certificación de la forma transitoria señalada en el punto anterior, exigiéndose a todas las entidades de certificación la acreditación recogida en el punto VI.1.

VI.4 Estarán exentas del cumplimiento de los requisitos señalados en los puntos anteriores del presente epígrafe aquellas entidades, órganos, organismos y unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias incluyan el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad.

VI.5 El Centro Criptológico Nacional mantendrá en su sede electrónica una relación actualizada de las Entidades de Certificación, acreditadas o en vías de acreditación, para expedir Certificaciones de Conformidad con el Esquema Nacional de Seguridad.

*VII. Soluciones y servicios prestados por el sector privado*

VII.1 Cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, utilizando los mismos procedimientos que los exigidos en esta Instrucción Técnica de Seguridad para las entidades públicas.

VIII.2 Es responsabilidad de las entidades públicas contratantes notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el Esquema Nacional de Seguridad y posean las correspondientes Declaraciones o Certificaciones de Conformidad, según lo señalado en la presente Instrucción Técnica de Seguridad.

VII.3 Cuando la provisión de las soluciones o la prestación de los servicios sujetos al cumplimiento del Esquema Nacional de Seguridad sean realizados por operadores del sector privado, estos utilizarán los mismos modelos documentales utilizados para las Declaraciones, las Certificaciones o los Distintivos de Conformidad recogidos en la presente Instrucción Técnica de Seguridad, sustituyendo las referencias a las entidades públicas por las correspondientes a las entidades privadas. Análogamente, los Distintivos de Conformidad, cuando se exhiban por parte de dichos operadores privados, deberán enlazar con las correspondientes Declaraciones o Certificaciones de Conformidad, que permanecerán siempre accesibles en la página electrónica del operador de que se trate.

VII.4 Además del Centro Criptológico Nacional y la Entidad Nacional de Acreditación, las entidades públicas usuarias de soluciones o servicios provistos o prestados por organizaciones del sector privado que exhiban una Declaración o Certificación de Conformidad con el Esquema Nacional de Seguridad podrán solicitar en todo momento a tales operadores los Informes de Autoevaluación o Auditoría correspondientes, al objeto de verificar la adecuación e idoneidad de las antedichas manifestaciones.

## ANEXO I

### Contenido de la Declaración de Conformidad con el Esquema Nacional de Seguridad

Cada entidad u organismo declarante podrá disponer libremente de su propio formato de Declaración de Conformidad con el Esquema Nacional de Seguridad, que deberá mostrar, al menos, el contenido siguiente:

– Logotipo de la entidad u organismo declarante.
– Identificación de la entidad u organismo declarante.
– Distintivo de Declaración de Conformidad de acuerdo al anexo II de esta Instrucción Técnica de Seguridad.
– Texto: “Declaración de Conformidad con el Esquema Nacional de Seguridad”.
– Texto: “Los sistemas de información reseñados, todos ellos de categoría BÁSICA, y los servicios que se relacionan, han superado un proceso de autoevaluación conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de <>:”

– <>.

– Texto: “Fecha de declaración de conformidad inicial: <> de <> de <>”
– Texto: “Fecha de renovación de la declaración de conformidad: <> de <> de <>”.
– Texto: “Fecha: <>, <> de <> de <>”.
– Firma: <>.

Los textos que aparecen entre paréntesis angulares se adaptarán a los aspectos concretos de la Declaración de Conformidad expedida.

La guía de seguridad CCN-STIC 809 sobre declaración y certificación de conformidad con el Esquema Nacional de Seguridad y distintivos de cumplimiento ofrecerá modelos ilustrativos de la citada Declaración de conformidad.

## ANEXO II

## Distintivo de Declaración de Conformidad con el Esquema Nacional de Seguridad


En la medida de lo posible, los Distintivos de Declaración de Conformidad con el Esquema Nacional de Seguridad que se exhiban en medios electrónicos o en papel respetarán las proporciones, formas, tipografía y colores de la imagen anterior.

| Colores directos | CMYK | RGB | Hexadecimal |
|---|---|---|---|
| Pantone Orange 021C | C: 0 | R: 235 | FF6600 |
| | M: 53 | G: 111 | |
| | Y: 100 | B: 12 | |
| | K: 0 | | |

## ANEXO III

### Contenido de la Certificación de Conformidad con el Esquema Nacional de Seguridad

Cada Entidad Certificadora podrá disponer libremente de su propio formato de Certificación de Conformidad con el Esquema Nacional de Seguridad, que deberá mostrar, al menos, el contenido siguiente:

– Logotipo de la Entidad Certificadora.
– Identificación de la Entidad Certificadora.
– Distintivo de Certificación de Conformidad de acuerdo al anexo IV de esta Instrucción Técnica de Seguridad.
– Texto: “Certificado de Conformidad con el Esquema Nacional de Seguridad”.
– Texto: “<> certifica que los sistemas de información reseñados, todos ellos de categoría <>, y los servicios que se relacionan, de <>, han sido auditados y encontrados conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de Auditoría de <>:”

– <>.

– Texto: “Número de certificado: <>”.
– Texto: “Fecha de certificación de conformidad inicial: <> de <> de <>”.
– Texto: “Fecha de renovación de la certificación de conformidad: <> de <> de <>”.
– Texto: “Fecha: <>, <> de <> de <>”.
– Firma: Nombre y Apellidos del responsable competente de la Entidad Certificadora.

Los textos que aparecen entre paréntesis angulares se adaptarán a los aspectos concretos de la certificación expedida.

La guía de seguridad CCN-STIC 809 sobre declaración y certificación de conformidad con el Esquema Nacional de Seguridad y distintivos de cumplimiento ofrecerá modelos ilustrativos de la citada Certificación de conformidad.

## ANEXO IV

### Distintivo de Conformidad con el Esquema Nacional de Seguridad


En la medida de lo posible, los Distintivos de Certificación de Conformidad con el Esquema Nacional de Seguridad que se exhiban en medios electrónicos o en papel respetarán las proporciones, formas, tipografía y colores de la imagen anterior.

| Colores directos | CMYK | RGB | Hexadecimal |
|---|---|---|---|
| Pantome 653C | C: 82 | R: 55 | 336699 |
| | M: 47 | G: 99 | |
| | Y: 11 | B: 150 | |
| | K: 0 | | |

# § 29

## Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información

Ministerio de Hacienda y Función Pública
«BOE» núm. 81, de 3 de abril de 2018
Última modificación: sin modificaciones
Referencia: BOE-A-2018-4573

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Dicho Real Decreto prevé, en su artículo 29, apartado 2, que el Ministerio de Hacienda y Función Pública, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante resolución de la Secretaría de Estado de Función Pública, constituyendo elementos esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el ENS.

Así pues, tales instrucciones técnicas de seguridad, enumeradas en la Disposición Adicional cuarta del citado Real Decreto 3/2010, de 8 de enero, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como: Informe del Estado de la Seguridad; Notificación de Incidentes de Seguridad; Auditoría de la Seguridad; Conformidad con el Esquema Nacional de Seguridad; Adquisición de Productos de Seguridad; Criptología de empleo en el Esquema Nacional de Seguridad; Interconexión en el Esquema Nacional de Seguridad y Requisitos de Seguridad en entornos externalizados, sin perjuicio de las propuestas que pueda acordar la Comisión Sectorial de administración electrónica, según lo establecido en el citado artículo 29, en relación con lo dispuesto en la Disposición derogatoria única de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y Disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Estas instrucciones técnicas de seguridad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

En particular, la instrucción técnica de seguridad de Auditoría de la Seguridad de los sistemas de información establece las condiciones para la realización de la preceptiva

auditoría a la que deben someterse los sistemas de información del ámbito de aplicación del ENS, tal y como se regula en el artículo 34 y Anexo III de su norma reguladora.

Por otra parte, de acuerdo con el Real Decreto 769/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Función Pública y se modifica el Real Decreto 424/2016, de 11 de noviembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales corresponde a la Secretaría de Estado de Función Pública el impulso, la programación y la supervisión de las actuaciones en ejecución de la política de Gobierno en materia de Administración Digital y del fomento de la administración electrónica, en especial lo referente al proceso de racionalización de las tecnologías de la información y de las comunicaciones, y la adopción de soluciones digitales que permitan la prestación eficiente de los servicios públicos incluyendo los servicios públicos esenciales.

Esta Resolución se aprueba en aplicación de lo dispuesto en el Real Decreto 3/2010, de 8 de enero, en el artículo 29, apartado 2, en el capítulo V, Auditoría de la seguridad, artículo 34, así como en su Anexo III, modificado por Real Decreto 951/2015, de 23 octubre, a propuesta de la Comisión Sectorial de Administración Electrónica.

En virtud de lo anterior, esta Secretaría de Estado resuelve:

**Primero.**

Aprobar la Instrucción Técnica de Seguridad «Auditoría de la Seguridad de los sistemas de información», cuyo texto se incluye a continuación.

**Segundo.**

Ordenar su publicación en el «Boletín Oficial del Estado».

La Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los sistemas de información que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE AUDITORÍA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

ÍNDICE



I. Objeto: La Instrucción Técnica de Seguridad de Auditoría de la Seguridad tiene por objeto establecer las condiciones para la realización de las auditorías, ordinarias o extraordinarias, previstas en el artículo 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

II. Ámbito de aplicación: La presente Instrucción Técnica de Seguridad será de aplicación a los sistemas de información comprendidos en los ámbitos subjetivo y objetivo de aplicación del Real Decreto 3/2010, de 8 de enero, según dispone el artículo 3 del mismo, así como al resto de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015,de 1 de octubre, de Régimen Jurídico del Sector Público.

III. Propósito de la Auditoría de la Seguridad, obligatoriedad y normativa reguladora:

III.1 La Auditoría de la Seguridad es un proceso sistemático, independiente y documentado, para la obtención de evidencias y su evaluación objetiva, con el fin de determinar el grado de conformidad con el ENS del sistema de información auditado. Debe

permitir a sus responsables adoptar las medidas oportunas para subsanar las deficiencias y atender a las observaciones o recomendaciones que pudiera haber identificado el Equipo Auditor y, en su caso, posibilitar la obtención de la correspondiente Certificación de Conformidad, tal y como dispone la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, regulada por Resolución de 13 de octubre de 2016, del Secretario de Estado de Administraciones Públicas.

III.2 Para obtener la Certificación de Conformidad con el ENS, los sistemas de información de categorías MEDIA o ALTA precisarán superar una Auditoría de Seguridad, al menos cada dos años. Los sistemas de información de categoría BÁSICA solo requerirán de una autoevaluación que, de ser favorable, permitirá la exhibición de la Declaración de Conformidad, y cuyo resultado deberá estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular, así como las evidencias que sustentan la valoración anterior. Dicha autoevaluación podrá ser desarrollada por el mismo personal que administra el sistema de información o en quién éste delegue.

III.3 Siendo obligatoria la Auditoría de Seguridad para los sistemas de categorías MEDIA o ALTA, nada impide que un sistema de categoría BÁSICA se someta asimismo a un proceso de Auditoría de Seguridad para la Certificación de la Conformidad, siendo siempre esta posibilidad la deseable.

III.4 El desarrollo de la Auditoría de la Seguridad se realizará con sujeción a la normativa contenida en la presente Instrucción Técnica de Seguridad y complementariamente, cuando corresponda, atendiendo a las normas nacionales e internacionales sobre auditoría de sistemas de información, entre ellas las guías CCN-STIC 802 Guía de auditoría, CCN-STIC 804 Guía de Implantación y CCN-STIC 808 Verificación del cumplimiento de las medidas en el ENS, y aquellas otras de ética y control de calidad interna de los auditores y entidades de auditoría, certificación y acreditación.

IV. Definición del alcance y objetivo de la Auditoría de la Seguridad:

IV.1 Los criterios metodológicos de auditoría utilizados, el alcance y objetivo de la Auditoría de la Seguridad deberán estar claramente definidos y documentados, conforme a lo dispuesto en el artículo 34 y en el Anexo III del ENS, debiendo aparecer en el Informe de Auditoría que se obtenga.

IV.2 Para asegurar la independencia objetiva de la Entidad Certificadora, las tareas de auditoría no incluirán en ningún caso la ejecución de acciones que puedan ser consideradas actividades de consultoría o similares, tales como implantación o modificación de aplicaciones, relacionadas con el sistema auditado, redacción de documentos requeridos por el ENS o procedimientos de actuación, así como recomendaciones particulares sobre productos o soluciones concretas, entre otros.

V. Ejecución de la Auditoría de la Seguridad:

V.1 La entidad titular del sistema de información a auditar facilitará a la Entidad Certificadora cuanta información fuera pertinente para realizar los trabajos de auditoría, teniendo en cuenta su alcance y las eventuales limitaciones derivadas del ordenamiento jurídico.

V.2 El Equipo Auditor está obligado a requerir y obtener las evidencias pertinentes para verificar los criterios de auditoría, cuya evaluación constituirán los hallazgos en que se basarán las conclusiones recogidas en el Informe de Auditoría.

VI. El Informe de Auditoría:

VI.1 Atendiendo a la categoría del sistema auditado (BÁSICA, MEDIA o ALTA) el dictamen sobre la conformidad con el ENS se basará en el cumplimiento de los preceptos contenidos en el RD 3/2010, de 8 de enero, y de las medidas de seguridad del Anexo II del ENS que resulten de aplicación, así como de aquellos requisitos específicos que pudieran documentarse en guías CCN-STIC en función del contexto interno o externo del sistema de información, identificando, en su caso, las desviaciones que se observen, así como los registros, declaraciones de hechos o cualquier otra información pertinente y verificable en que se basen las conclusiones alcanzadas.

VI.2 Los hallazgos de no conformidad se clasificarán atendiendo a los siguientes grados:

– «No Conformidad Menor»: Se documentará una «No Conformidad Menor» ante la ausencia o el fallo en la implantación o mantenimiento de uno o más de los requisitos del ENS, incluyendo cualquier situación que pudiese, en base a una evidencia objetiva, sustentar una duda significativa sobre la conformidad del sistema de información con uno o más de tales requisitos.

– «No Conformidad Mayor»: Se documentará una «No Conformidad Mayor» cuando se detecten «No Conformidades Menores» en relación con cualquiera de los preceptos contenidos en el RD 3/2010, de 8 de enero, o en el Marco organizativo, o en alguno de los subgrupos que integran el Marco operacional o las Medidas de protección (Planificación, Control de Accesos, Explotación, Servicios Externos, Continuidad del Servicio, Monitorización del Sistema, Protección de las Infraestructuras, Gestión del Personal, Protección de Equipos, Comunicaciones, Soportes de Información, Aplicaciones Informáticas, Información o Servicios) que, evaluadas en su conjunto, puedan implicar el incumplimiento del objetivo del Grupo o Subgrupo considerados.

Se documentará una Observación cuando se encuentren evidencias de una debilidad, una vulnerabilidad o una situación que, sin comprometer cualquier área del sistema de gestión definida en el ENS o por la organización, pueda, en la actualidad o en el futuro, derivar en un problema.

VI.3 El dictamen final de la Auditoría de la Seguridad será uno de los tres siguientes:

– «FAVORABLE»: Cuando no se evidencie ninguna «No Conformidad Mayor» o «No Conformidad Menor».

– «FAVORABLE CON NO CONFORMIDADES»: Cuando se evidencie cualquier no conformidad, mayor o menor. En este caso, la entidad titular responsable del sistema de información auditado deberá presentar, en el plazo máximo de un mes, un Plan de Acciones Correctivas sobre tales hallazgos de no conformidad a la entidad certificadora para su evaluación.

– «DESFAVORABLE»: Cuando, por el número o la transcendencia de las no conformidades detectadas, no sea posible decidir sobre su resolución a través de un Plan de Acciones Correctivas. En este caso se requerirá la realización de una auditoría extraordinaria que verifique la adopción de las medidas correctoras adecuadas.

La Guía CCN-STIC 824 Informe del Estado de Seguridad, que el Centro Criptológico Nacional mantendrá permanentemente actualizada, ofrecerá pautas de ayuda para el dictamen final de la Auditoría de la Seguridad.

VI.4 La Certificación de Conformidad con el ENS únicamente podrá expedirse si el dictamen fuera «FAVORABLE» o, si habiendo sido «FAVORABLE CON NO CONFORMIDADES», el Plan de Acciones Correctivas presentado por la entidad titular del sistema de información, trata y resuelve los hallazgos de no conformidad evidenciados, a criterio de la entidad certificadora.

VI.5 Ante un dictamen «DESFAVORABLE», la entidad titular del sistema de información auditado, en un plazo no superior a seis meses desde la fecha de emisión del Informe de Auditoría, deberá someterse a una Auditoría Extraordinaria, exclusivamente sobre los hallazgos de no conformidad evidenciados que, de resultar satisfactorio, permitirá la expedición del correspondiente Certificado de Conformidad con el ENS.

VI.6 En caso de un sistema certificado sobre el que se detecten No Conformidades Mayores, durante el período de resolución de las No Conformidades Mayores el Certificado de Conformidad quedará en suspenso. En caso de no cerrar las No Conformidades Mayores en un plazo de seis meses el Certificado de Conformidad quedaría revocado y la entidad auditada deberá eliminar el Distintivo de Conformidad de su sede hasta su próxima recertificación.

VI.7 El informe de Auditoría deberá contener la información adecuada y suficiente para facilitar y justificar la decisión de certificación, como mínimo:

– Las áreas organizativas, módulos o funciones del sistema de información cubiertas por la auditoría, incluyendo los requisitos de certificación y las ubicaciones que fueron auditadas, las pistas de auditoría seguidas y las metodologías de auditoría utilizadas.

– Los hallazgos identificados, tanto de conformidad como de no conformidad, incluyendo las Observaciones.

– Los detalles de las no conformidades identificadas se justificarán mediante evidencias objetivas y su correspondencia con los requisitos del ENS u otros documentos requeridos para la Certificación.

– Comentarios sobre la conformidad del Sistema de Gestión de Seguridad de la Información del auditado con los requisitos de certificación, con una redacción clara de las no conformidades que hubieran podido evidenciarse, una referencia a la versión de la Declaración de Aplicabilidad, que incluya el nivel en cada dimensión para cada medida de seguridad del ENS aplicable, así como cualquier comparación útil con los resultados de Auditorías de la Seguridad previas.

– La Categoría del Sistema, con detalle del nivel de seguridad en cada una de las dimensiones recogidas en el ENS.

– El grado de confianza en las revisiones de la Dirección y auditorías internas del auditado.

– La conclusión o dictamen del Equipo de Auditoría sobre si el sistema de información del auditado debe ser certificado o no, con información que soporte esa conclusión.

VI.8 Los informes de auditoría podrán ser requeridos por el CCN-CERT, en los términos previstos en el artículo 37 del ENS.

VII. Entidades Auditoras del Sector Público: La presente Instrucción Técnica de Seguridad también será de aplicación a las actividades de auditoría y a la emisión de los correspondientes informes que se realicen por entidades, órganos, organismos y unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias se correspondan con el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad.

VIII. Disposición adicional. Datos personales:

VIII.1 Cuando el sistema auditado tenga por objeto o incluya el tratamiento de datos personales se tendrá en cuenta lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

VIII.2 A partir del 25 de mayo de 2018, cuando el sistema auditado tenga por objeto o incluya el tratamiento de datos personales, se tendrá en cuenta el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. A partir de dicha fecha en todo momento se informará al Delegado de Protección de Datos en calidad de responsable de la supervisión del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

# § 30

## Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad

Ministerio de Hacienda y Función Pública
«BOE» núm. 95, de 19 de abril de 2018
Última modificación: sin modificaciones
Referencia: BOE-A-2018-5370

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, ENS en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Dicho Real Decreto prevé, en su artículo 29, apartado 2, que el Ministerio de Hacienda y Función Pública, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante resolución de la Secretaría de Estado de Función Pública, constituyendo elementos esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el ENS.

Así pues, tales instrucciones técnicas de seguridad, enumeradas en la Disposición Adicional cuarta del citado Real Decreto 3/2010, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como: Informe del Estado de la Seguridad; Notificación de Incidentes de Seguridad; Auditoría de la Seguridad; Conformidad con el Esquema Nacional de Seguridad; Adquisición de Productos de Seguridad; Criptología de empleo en el Esquema Nacional de Seguridad; Interconexión en el Esquema Nacional de Seguridad y Requisitos de Seguridad en entornos externalizados, sin perjuicio de las propuestas que pueda acordar la Comisión Sectorial de administración electrónica, según lo establecido en el citado artículo 29, en relación con lo dispuesto en la Disposición derogatoria única de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y Disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Estas instrucciones técnicas de seguridad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

En particular, la instrucción técnica de seguridad de Notificación de Incidentes de Seguridad establece los criterios y procedimientos para la notificación por parte de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público al Centro Criptológico Nacional (CCN) de aquellos incidentes que tengan un impacto significativo en la seguridad de la información que manejan y los servicios que prestan en relación con la categoría del sistema, al objeto de poder dar adecuada respuesta al mandato del Capítulo VII, Respuesta a incidentes de seguridad, del Real Decreto 3/2010, de 8 de enero.

Por otra parte, de acuerdo con el Real Decreto 769/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Función Pública y se modifica el Real Decreto 424/2016, de 11 de noviembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales corresponde a la Secretaría de Estado de Función Pública el impulso, la programación y la supervisión de las actuaciones en ejecución de la política de Gobierno en materia de Administración Digital y del fomento de la administración electrónica, en especial lo referente al proceso de racionalización de las tecnologías de la información y de las comunicaciones, y la adopción de soluciones digitales que permitan la prestación eficiente de los servicios públicos incluyendo los servicios públicos esenciales. Además, dado que la resolución impone obligaciones no solo en el ámbito competencial de esta Secretaria de Estado sino también al Centro Criptológico Nacional (CCN) integrado en el CNI, organismo adscrito al Ministerio de la Presidencia y para las Administraciones Territoriales procede recabar el parecer del citado Departamento.

Esta Resolución se aprueba en aplicación de lo dispuesto en el artículo 29, apartado 2 del Real Decreto 3/2010, de 8 de enero, a propuesta de la Comisión Sectorial de Administración Electrónica y habiéndose solicitado informe al Ministerio de la Presidencia y para las Administraciones Territoriales.

En virtud de lo anterior, esta Secretaría de Estado resuelve:

**Primero.**

Aprobar la Instrucción Técnica de Seguridad «Notificación de incidentes de seguridad», cuyo texto se incluye a continuación.

**Segundo.**

Ordenar su publicación en el «Boletín Oficial del Estado».

La Instrucción Técnica de Seguridad de Notificación de incidentes de seguridad de los sistemas de información que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

ÍNDICE



### *I. Objeto*

La Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad tiene por objeto, según lo dispuesto en el Capítulo VII del Real Decreto 3/2010, de 8 de enero, la notificación y gestión de incidentes de seguridad en los sistemas de información de las entidades del Sector Público del ámbito de aplicación de dicho cuerpo legal, cuando tales

incidentes tengan un impacto significativo en la seguridad de la información que manejan o los servicios que prestan, en relación con la categoría del sistema y con independencia de los requerimientos adicionales que cada organismo o entidad implemente para adaptarlos a sus entornos singulares.

*II. Ámbito de aplicación*

La presente Instrucción Técnica de Seguridad será de aplicación a los sistemas de información comprendidos en los ámbitos subjetivo y objetivo de aplicación del Real Decreto 3/2010, de 8 de enero, según dispone el artículo 3 del mismo, así como al resto de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

*III. Criterios de determinación del nivel de Impacto*

Una vez detectado un incidente se utilizará la Guía CCN-STIC 817 Esquema Nacional de Seguridad - Gestión de Ciberincidentes, para clasificarlo de acuerdo con su tabla Criterios de determinación del nivel de impacto potencial. El nivel de impacto potencial de los ciberincidentes en la organización, será: Irrelevante, Bajo, Medio, Alto, Muy Alto y Crítico.

*IV. Notificación obligatoria de los incidentes con nivel de impacto Alto, Muy alto y Crítico*

IV.1 Las notificaciones efectuadas por las entidades del ámbito de aplicación de la presente Instrucción Técnica de Seguridad al Centro Criptológico Nacional (CCN), en el marco de la articulación de respuesta a los incidentes de seguridad y la prestación de servicios de respuesta por parte del Equipo de Respuesta a Incidentes de Seguridad del CCN-CERT, (Centro Criptológico Nacional - Computer Emergency Response Team) se realizará en los términos indicados en los artículos 36 y 37 del Real Decreto 3/2010, de 8 de enero.

IV.2 Para ello, se notificarán los incidentes de seguridad que tengan un impacto significativo en la seguridad de la información manejada o los servicios prestados en relación con la categoría del sistema, determinada de acuerdo con lo dispuesto en los artículos 43, 44 y Anexo I del Real Decreto 3/2010, de 8 de enero. Se dice que un incidente tiene impacto significativo cuando, por su magnitud o características, impide el tratamiento de la información o los servicios prestados. A estos efectos, se considerará que tienen un impacto significativo los niveles Alto, Muy Alto y Crítico recogidos en la tabla Criterios de Determinación del Nivel de Impacto de la Guía CCN-STIC 817.

IV.3 En todo caso, serán de obligatoria notificación al CCN en el momento en que se produzcan, los incidentes de seguridad que por su nivel de impacto potencial sean calificados con el nivel de CRÍTICO, MUY ALTO o ALTO, mediante el empleo de las herramientas desarrolladas al efecto de la notificación de incidentes.

*V. Evidencias a entregar en el caso de incidentes nivel Alto, Muy alto y Crítico*

V.1 Tras la detección de un incidente de seguridad y con carácter inmediato se recopilarán evidencias del incidente, que serán documentadas y custodiadas de forma que se pueda determinar el modo de obtención, se garantice la cadena de custodia, y respetando el ordenamiento jurídico que resulte de aplicación. En la recolección y custodia de evidencia se aplicarán las recomendaciones establecidas al efecto en la Guía CCN-STIC 817.

V.2 De acuerdo con lo dispuesto en el artículo 37 del Real Decreto 3/2010, de 8 de enero, el CCN podrá recabar éstas y cualesquiera otras informaciones que se consideren relevantes para el análisis del incidente, así como los soportes informáticos que se estimen necesarios para la investigación, sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y su normativa de desarrollo, así como la posible confidencialidad de datos de carácter institucional u organizativo.

*VI. Obligación de remisión de estadísticas de incidentes*

De conformidad con lo dispuesto en el artículo 24.2 del Real Decreto 3/2010, de 8 de enero, el registro de todos los incidentes de seguridad que se produzcan y de las acciones de tratamiento que se sigan, será utilizado para la mejora continua de la seguridad del sistema, a cuyo fin las entidades del ámbito de aplicación de la presente Instrucción Técnica de Seguridad elaborarán estadísticas de incidentes de seguridad que, al menos, con carácter anual, remitirán al CCN, incluyendo el resto de la antedicha información relativa a los incidentes.

*VII. Notificación de impactos recibidos*

Una vez determinado el impacto del ciberincidente y calificado como de carácter significativo a los efectos de lo establecido en el artículo 36 del ENS, será notificado al CCN en los términos previsto en el artículo IV de la presente Instrucción Técnica de Seguridad.

*VIII. Desarrollo de herramientas automatizadas para facilitar las notificaciones*

El CCN ha desarrollado la herramienta LUCIA, Listado Unificado de Coordinación de Incidentes y Amenazas) con el propósito de automatizar los mecanismos de notificación, comunicación e intercambio de información sobre incidentes de seguridad, de acuerdo a lo establecido en la Guía CCN-STIC 817. Esta herramienta se mantendrá permanentemente actualizada para atender dicho propósito.

*IX. Régimen legal de las notificaciones y comunicación de información*

Para la articulación de respuesta a los incidentes de seguridad y gestión de ciberincidentes a los que se refiere la presente Resolución, el suministro de información por las entidades del ámbito de aplicación de la presente Instrucción Técnica de Seguridad al CCN, motu proprio o a su requerimiento, se realizará teniendo en cuenta lo siguiente:

a) La comunicación de información que tenga la consideración de datos de carácter personal se efectuará con pleno cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y su normativa de desarrollo, atendiendo a que la comunicación de datos se realiza para el cumplimiento de fines directamente relacionados con la función legítima de las entidades cedentes y del CCN como cesionario, sin que sea preciso el consentimiento del afectado toda vez que tales datos han sido recabados para el ejercicio de las funciones propias de unos y otro, en los términos previstos en el artículo 6.2 de la citada Ley Orgánica.

Tampoco resultará de aplicación lo dispuesto en los párrafos uno y dos del artículo 5 de la reiterada Ley Orgánica, en base a lo dispuesto en su artículo 24.1, por afectar a la Ciberseguridad, como ámbito de especial interés para la Seguridad Nacional.

b) La comunicación de información de datos de carácter institucional u organizativo a la que se refiere el artículo 37.1.a) último párrafo, del Real Decreto 3/2010, de 8 de enero, será suministrada y comunicada en función de su confidencialidad, atendiendo a lo dispuesto en el artículo 43 y anexo I, en relación con el citado artículo 37.1.a) del ENS.

*X. Disposición adicional*

X.1 Las referencias contenidas en la presente Instrucción a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo se entenderán hechas, a partir del 25 de mayo de 2018, al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

X.2 Se añade un segundo párrafo al apartado VII de la Instrucción, con efectos a partir del 25 de mayo de 2018, con la siguiente redacción:

> «Cuando el incidente afecte a datos personales la notificación a la autoridad de control competente se realizará con independencia del nivel de impacto del incidente

en el Esquema Nacional de Seguridad. En aquellos casos en los que el impacto de un incidente o violación de la seguridad afecte a datos personales, la notificación se realizará según lo previsto en el artículo 33 del Reglamento General de Protección de Datos.»

X.3 La referencia contenida en el apartado IX, letra a), primer párrafo, de la Instrucción, al artículo 6.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se entenderá realizada, a partir del 25 de mayo de 2018, al artículo 6.1.c) del Reglamento General de Protección de Datos.

X.4 La referencia contenida en el apartado IX, letra a), segundo párrafo, a «los párrafos uno y dos del artículo 5 de la reiterada Ley Orgánica, en base a lo dispuesto en su artículo 24.1», se entenderá sustituida, a partir del 25 de mayo de 2018, por «el capítulo III del Reglamento General de Protección de Datos, en base a lo dispuesto en el artículo 23.1.a) del mismo».

# § 31

## Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional

Ministerio de Defensa
«BOE» núm. 68, de 19 de marzo de 2004
Última modificación: sin modificaciones
Referencia: BOE-A-2004-5051

La sociedad española demanda unos servicios de inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional.

Entre los elementos más característicos de esta nueva situación figuran el desarrollo alcanzado por las tecnologías de la información, la facilidad y flexibilidad de su transmisión en diversos soportes, la generalización casi universal de su uso y la accesibilidad global a las diversas herramientas y redes. Todos estos rasgos facilitan el intercambio ágil y flexible de información en las sociedades modernas.

Al mismo tiempo, la elaboración, conservación y utilización de determinada información por parte de la Administración es necesaria para garantizar su funcionamiento eficaz al servicio de los intereses nacionales.

En consecuencia, la Administración debe dotarse de los medios adecuados para la protección y control del acceso a dicha información, y ha de regular unos procedimientos eficaces para su almacenamiento, procesamiento y transmisión seguros por medio de sistemas propios.

Razones de eficacia, economía y coherencia administrativa recomiendan el establecimiento de medidas para regular y coordinar la adquisición del sofisticado material que se precisa, la homologación de su capacidad y compatibilidad, sus procedimientos de empleo y la formación técnica del personal de la Administración especialista en este campo. Asimismo, ha de elaborarse y mantenerse actualizada la normativa relativa a la protección de la información clasificada y velar por su cumplimiento, para evitar el acceso a ésta de individuos, grupos y Estados no autorizados.

El concepto de seguridad de los sistemas de información no sólo abarca la protección de la confidencialidad de ésta; en la mayoría de los casos es necesario también que los sistemas permitan el acceso de los usuarios autorizados, funcionen de manera íntegra y garanticen que la información que manejan mantiene su integridad. En consecuencia, la seguridad de los sistemas de información debe garantizar la confidencialidad, la disponibilidad y la integridad de la información que manejan y la disponibilidad y la integridad de los propios sistemas.

Se hace necesaria la participación de un organismo que, partiendo de un conocimiento de las tecnologías de la información y de las amenazas y vulnerabilidades que existen, proporcione una garantía razonable sobre la seguridad de productos y sistemas. A partir de

esa garantía, los responsables de los sistemas de información podrán implementar los productos y sistemas que satisfagan los requisitos de seguridad de la información.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Este real decreto se dicta en virtud de lo dispuesto en la disposición final primera de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

En su virtud, a propuesta del Ministro de Defensa, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 12 de marzo de 2004,

DISPONGO:

**Artículo 1.** *Del Director del Centro Criptológico Nacional.*

El Secretario de Estado Director del Centro Nacional de Inteligencia, como Director del Centro Criptológico Nacional (CCN), es la autoridad responsable de coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada del material criptológico y formar al personal de la Administración especialista en este campo. En este sentido, el Director del CCN es la autoridad de certificación de la seguridad de las tecnologías de la información y autoridad de certificación criptológica.

Asimismo es responsable de velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en los aspectos de los sistemas de información y telecomunicaciones, de acuerdo a lo señalado en el artículo 4.e) y f) de la Ley 11/2002, de 6 de mayo.

**Artículo 2.** *Del ámbito de actuación y funciones del Centro Criptológico Nacional.*

1. El ámbito de actuación del Centro Criptológico Nacional comprende:

a) La seguridad de los sistemas de las tecnologías de la información de la Administración que procesan, almacenan o transmiten información en formato electrónico, que normativamente requieren protección, y que incluyen medios de cifra.

b) La seguridad de los sistemas de las tecnologías de la información que procesan, almacenan o transmiten información clasificada.

2. Dentro de dicho ámbito de actuación, el Centro Criptológico Nacional realizará las siguientes funciones:

a) Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración. Las acciones derivadas del desarrollo de esta función serán proporcionales a los riesgos a los que esté sometida la información procesada, almacenada o transmitida por los sistemas.

b) Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y las comunicaciones.

c) Constituir el organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito.

d) Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura.

e) Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas antes mencionados.

f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.

g) Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

Para el desarrollo de estas funciones, el CCN podrá establecer la coordinación oportuna con las comisiones nacionales a las que las leyes atribuyan responsabilidades en el ámbito de los sistemas de las tecnologías de la información y de las comunicaciones.

3. El Centro Criptológico Nacional queda adscrito al Centro Nacional de Inteligencia y comparte con éste medios, procedimientos, normativa y recursos, y se regirá por la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. El personal del CCN estará integrado orgánica y funcionalmente en el Centro Nacional de Inteligencia, por lo que le serán de aplicación todas las disposiciones relativas al personal de éste, contempladas en la Ley 11/2002, de 6 de mayo, y en la normativa de desarrollo, particularmente su régimen estatutario.

**Disposición derogatoria única.** *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

**Disposición final primera.** *Facultades de desarrollo.*

Se faculta al Ministro de Defensa para dictar cuantas disposiciones sean necesarias para la aplicación y el desarrollo de lo establecido en este real decreto.

**Disposición final segunda.** *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

# § 32

## Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021

Presidencia del Gobierno
«BOE» núm. 314, de 31 de diciembre de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-21884

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, establece que la política de Seguridad Nacional es una política pública, en la que bajo la dirección del Presidente del Gobierno y la responsabilidad del Gobierno, participan todas las administraciones públicas, de acuerdo con sus respectivas competencias, y la sociedad en general, para responder a las necesidades de la Seguridad Nacional.

Para materializar esta visión inclusiva del conjunto de los componentes del sector público, del sector privado y de la sociedad en su conjunto en la plasmación de la política de Seguridad Nacional, la citada ley prevé que la Estrategia de Seguridad Nacional se configure como el marco político estratégico de referencia de la Política de Seguridad Nacional. Asimismo, prevé que contendrá el análisis del entorno estratégico, la concreción de los riesgos y amenazas que afectan a la seguridad de España, la definición de las líneas de acción estratégicas en cada ámbito de actuación y la promoción de la optimización de los recursos existentes.

A nivel procedimental, establece que será elaborada a iniciativa del Presidente del Gobierno, quien la someterá a la aprobación del Consejo de Ministros, y se revisará cada cinco años o cuando lo aconsejen las circunstancias cambiantes del entorno estratégico. Una vez aprobada, será presentada en las Cortes Generales y, en concreto, en la Comisión Mixta Congreso-Senado de Seguridad Nacional.

En el año 2011 se aprobó la primera Estrategia Española de Seguridad al término de la IX Legislatura, sin margen temporal para su desarrollo.

En la X Legislatura, y tras la adecuación de la estructura de la Presidencia del Gobierno que dio carta de naturaleza a la creación del Departamento de Seguridad Nacional, por Real Decreto 1119/2012, de 20 de julio, se procedió a la revisión de la Estrategia de 2011, que tras un proceso de amplio espectro, consensuado a nivel político y abierto a la sociedad, cristalizó el 31 de mayo de 2013 en una nueva Estrategia de Seguridad Nacional, estrategia que fue sustituida por la aprobada a propuesta del Presidente del Gobierno y previa deliberación del Consejo de Ministros en su reunión del día 1 de diciembre de 2017, vigente actualmente.

El Presidente del Gobierno consideró que las circunstancias cambiantes, planteadas en España y en el mundo en general por la situación de la pandemia de la COVID-19 hacían necesario adelantar el periodo de renovación de la Estrategia de Seguridad Nacional vigente desde el año 2017 y, en la reunión del Consejo de Seguridad Nacional del 22 de junio de 2020, dio el mandato de iniciar la elaboración de una nueva estrategia, ahora materializada.

A iniciativa del Presidente del Gobierno, el Consejo de Seguridad Nacional celebrado el día 6 de octubre de 2020 adoptó el Acuerdo por el que se aprueba el procedimiento para la elaboración de la Estrategia de Seguridad Nacional 2021, y que ha sido elaborada de acuerdo con las previsiones de la Ley de Seguridad Nacional.

Las motivaciones que han impulsado la revisión de la vigente Estrategia se centran en la necesidad de adaptarla a la cambiante situación de los ámbitos de la Seguridad Nacional, sin olvidar el importante cambio operado por la pandemia de la COVID-19, que obligan a todos los poderes públicos a profundizar en la forma de garantizar los derechos y el bienestar de los ciudadanos, garantizando la defensa de España y sus principios y valores constitucionales.

El texto de la nueva Estrategia, elaborado de conformidad con el procedimiento aprobado en el acuerdo antes mencionado, ha sido sometido a informe favorable del Consejo de Seguridad Nacional en su reunión celebrada el día 18 de noviembre de 2021.

La aprobación de la Estrategia corresponde al Gobierno mediante real decreto según dispone el artículo 14.b) de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, a propuesta del Presidente del Gobierno, según lo establecido en el artículo 15.b) del mismo texto legal.

En su virtud, a propuesta del Presidente del Gobierno, y previa deliberación del Consejo de Ministros en su reunión del día 28 de diciembre de 2021,

DISPONGO:

**Artículo único.** *Aprobación de la Estrategia de Seguridad Nacional 2021.*

Se aprueba la Estrategia de Seguridad Nacional 2021, la cual se configura como el marco político-estratégico de referencia de la política de Seguridad Nacional, y cuyo texto se incluye a continuación.

**Disposición derogatoria única.** *Derogación normativa.*

Queda derogado el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017.

**Disposición final primera.** *Títulos competenciales.*

Este real decreto se dicta al amparo de los títulos competenciales previstos en el artículo 149.1.4.ª y 29.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de Defensa y Fuerzas Armadas y en materia de seguridad pública, respectivamente.

**Disposición final segunda.** *Habilitación para el desarrollo reglamentario.*

Se autoriza al Gobierno para dictar cuantas disposiciones sean necesarias para el desarrollo de este real decreto.

**Disposición final tercera.** *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## ESTRATEGIA DE SEGURIDAD NACIONAL 2021

El Consejo de Seguridad Nacional ha sido el órgano responsable de la elaboración de la Estrategia de Seguridad Nacional 2021, en cuyo proceso han participado los departamentos ministeriales y el Centro Nacional de Inteligencia.

También han participado las Comunidades y Ciudades Autónomas a través de la Conferencia Sectorial para Asuntos de Seguridad Nacional.

La Estrategia de Seguridad Nacional 2021 incluye asimismo las aportaciones de expertos independientes, personas de reconocido prestigio, conocimientos y experiencia en el campo de la seguridad.

La coordinación del proceso ha sido llevada a cabo por el Departamento de Seguridad Nacional del Gabinete de la Presidencia del Gobierno en su condición de Secretaría Técnica y Órgano de Trabajo Permanente del Consejo de Seguridad Nacional.

RESUMEN EJECUTIVO

La Estrategia de Seguridad Nacional 2021 se estructura en cinco capítulos.

El primer capítulo, titulado «Seguridad Global y Vectores de Transformación», analiza el contexto internacional de seguridad. La Estrategia identifica la pandemia de la COVID-19 como un factor que ha producido una aceleración de las principales dinámicas globales que afectan a la seguridad. Sin poder afirmar categóricamente que se trata de un cambio de era, sí que se percibe el momento actual como etapa de transición. La característica predominante es la incertidumbre sobre un futuro donde la transformación digital y la transición ecológica se configuran como las principales palancas de cambio en un escenario de mayor competición geopolítica.

El segundo capítulo, «Una España Segura y Resiliente», traza un perfil de España y su seguridad. Desde su identificación como país de condición europea, mediterránea y atlántica, se realiza un recorrido geográfico, donde Europa, Magreb y Oriente Próximo, África Subsahariana, América del Norte, América Latina y el Caribe, y Asia-Pacífico se analizan desde el prisma de la Seguridad Nacional.

El tercer capítulo recoge los riesgos y las amenazas a la Seguridad Nacional, cuyas principales características son su interrelación y dinamismo. De esta forma, el seguimiento de las conexiones entre riesgos resulta tan importante como su análisis de forma independiente. La principal actualización en el mapa de riesgos es la inclusión de las campañas de desinformación. Además, la tecnología y las estrategias híbridas son elementos transversales al conjunto de riesgos y amenazas a la Seguridad Nacional.

El cuarto capítulo, titulado «Un Planeamiento Estratégico Integrado», establece tres objetivos, que marcan las prioridades de la Seguridad Nacional para este ciclo estratégico. El primer objetivo es avanzar en materia de gestión de crisis; el segundo objetivo es favorecer la dimensión de la seguridad de las capacidades tecnológicas y los sectores estratégicos; y el tercer objetivo es desarrollar la capacidad preventiva, de detección y respuesta frente a las estrategias híbridas.

A continuación, la Estrategia traza tres ejes –proteger, promover y participar– sobre los que se estructuran las líneas de acción. Este planteamiento otorga especial relevancia al avance en la integración del Sistema de Seguridad Nacional y a la acción frente a situaciones de crisis. A los efectos de articular una política preventiva, se identifica como área clave el establecimiento de un sistema de alerta temprana, sobre una base tecnológica, que proporcione indicadores para todos los ámbitos de la Seguridad Nacional.

La Estrategia de Seguridad Nacional 2021 plantea iniciativas necesarias, como por ejemplo, la creación de una reserva estratégica basada en capacidades nacionales de producción industrial o el desarrollo de un plan integral de seguridad para Ceuta y Melilla.

En el plano internacional, España apuesta por una mayor autonomía estratégica europea, donde al impulso de la Política Común de Seguridad y Defensa y del espacio de libertad, seguridad y justicia se unen la mejora de la seguridad sanitaria, el avance en la unión energética o el mayor protagonismo de la Unión Europea en la gestión de crisis transfronterizas. Además, en materia de seguridad colectiva, la revisión estratégica de la OTAN supondrá un hito importante, que incluirá la colaboración con la Unión Europea como una de sus líneas de acción.

Finalmente, el quinto capítulo está dedicado a la gestión de crisis en el marco del Sistema de Seguridad Nacional, con un enfoque que parte de una visión del principio de resiliencia que incluye la progresión desde una situación de normalidad hasta la recuperación después de una situación de crisis. El avance en la integración del Sistema se materializa en actuaciones concretas. La primera de ellas es la elaboración de un catálogo de recursos de la Seguridad Nacional. La segunda es la preparación de planes de respuesta para determinados escenarios. La tercera es el desarrollo de un sistema de alerta temprana y análisis con indicadores que faciliten la toma de decisiones basada en datos objetivos concretos. La cuarta medida hace referencia a la integración de la información de la Seguridad Nacional a través de soluciones tecnológicas. La mejora de las comunicaciones

especiales de la Presidencia del Gobierno es la quinta medida, que contribuirá a la eficiencia del Sistema de Seguridad Nacional, al permitir una mayor coordinación entre administraciones en materia de gestión de crisis. La sexta y última medida contempla la integración de las Comunidades y Ciudades Autónomas en el Sistema de Seguridad Nacional.

## INTRODUCCIÓN

En condiciones normales, la revisión de la Estrategia de Seguridad Nacional 2017 hubiese llevado a cabo pasados cinco años. Sin embargo, el impacto de la pandemia de la COVID-19 y el incremento en el empleo de estrategias híbridas han aconsejado una revisión estratégica que permita enfrentar los riesgos y las amenazas en un renovado contexto de globalización, condicionado por una mayor incertidumbre y un cambio acelerado.

La pandemia ha sido el evento con mayor impacto global desde la Segunda Guerra Mundial, con grave afectación a la salud, la economía y la seguridad. Aun cuando se hayan superado todos sus efectos, perdurará la interdependencia del mundo actual, que contribuye a generar vulnerabilidades y a menudo actúa como factor multiplicador de las amenazas a medio y a largo plazo. Las pandemias, el cambio climático, los ciberataques o las crisis financieras son todos riesgos y amenazas complejas, a menudo interconectadas, que pueden desencadenar crisis en cascada.

En particular, los efectos del cambio climático pueden agudizar crisis económicas, políticas y geopolíticas derivadas de la escasez alimentaria e hídrica en muchas partes del mundo. Como consecuencia, podrían agravarse las situaciones de migraciones masivas, inestabilidad regional e incluso producirse nuevos conflictos armados. Asimismo, el calentamiento global tendrá repercusiones directas en España, pues provocará fenómenos meteorológicos adversos más extremos y frecuentes, sequías, olas de calor, inundaciones, escasez de agua y perjuicios para la biodiversidad.

Por otra parte, como muestra la realidad de los últimos años, el uso de estrategias híbridas por parte de actores estatales y no estatales como herramienta para presionar a los gobiernos democráticos es cada vez más frecuente.

A la hora de responder a las amenazas globales se plantea un dilema entre el repliegue estratégico de los Estados como forma de protección y la necesaria colaboración e intercambio de información entre países y organizaciones para buscar soluciones conjuntas. Este dilema paradigmático dificulta la articulación de respuestas en el marco de las organizaciones internacionales.

Por eso, ante futuras amenazas y crisis globales, será importante invertir esfuerzos en reforzar un sistema multilateral universal y regional que sea capaz de responder de forma coordinada y efectiva. En este sentido, y a la luz de la experiencia en Afganistán, la Unión Europea debe efectuar acciones conjuntas militares que contribuyan a reforzar el vínculo trasatlántico y que favorezcan la gestión de crisis transfronterizas y su autonomía estratégica. En particular, la Unión Europea debe asumir un mayor papel a la hora de gestionar desafíos, como las pandemias, el terrorismo internacional, los ciberataques o las campañas de desinformación, que requieren respuestas colectivas y la integración de capacidades.

La magnitud de los riesgos y las amenazas actuales requiere la correcta adecuación de los recursos, medios, sistemas y organizaciones disponibles para hacerles frente. La pandemia ha puesto de relieve la importancia de los sistemas de alerta temprana, de la fusión y el análisis de la información y de los planes de respuesta para la gestión de crisis, medidas todas ellas que facilitan y agilizan la toma de decisiones. Para ello, es necesario disponer de un Sistema de Seguridad Nacional digitalizado, capaz de proporcionar datos para la toma de decisiones en tiempo oportuno.

La prevención y la adaptación serán las claves para lograr un Sistema de Seguridad Nacional eficiente. Esto requiere:

Más anticipación: La Estrategia de Seguridad Nacional debe orientar la implantación de un sistema de alerta temprana y la preparación de planes de gestión de crisis. Todo ello con la participación de las Comunidades Autónomas, ya que numerosos recursos y capacidades de detección y gestión están entre sus competencias transferidas.

Más integración: La visión integral de la Seguridad Nacional requiere la necesaria coordinación del conjunto de las Administraciones Públicas y recursos del Estado, la colaboración público-privada y la implicación de la ciudadanía.

Más resiliencia: Para reducir la vulnerabilidad es tan necesario mitigar riesgos como robustecer la resiliencia, es decir, la capacidad de resistencia, transformación y recuperación ante una situación adversa.

Además, para gestionar futuras crisis y poder contar con los recursos críticos necesarios, es importante asegurar que las cadenas de suministro de estos recursos no dependan excesivamente del exterior. Asimismo, esto contribuirá a contener la expansión de las crisis, al fortalecer la resiliencia de la sociedad y de la economía.

## CAPÍTULO 1

### Seguridad global y vectores de transformación

El primer capítulo de la Estrategia de Seguridad Nacional describe el contexto internacional de seguridad y traza las principales dinámicas de transformación.

El orden global y el paradigma socio-económico liberal se encuentran en un periodo de cambio, sin que aún se haya definido claramente el nuevo panorama del sistema internacional. Los principales vectores de transformación son: el contexto geopolítico, el entorno socio-económico, la transformación digital y la transición ecológica.

#### *Contexto geopolítico*

El escenario geopolítico global se encuentra en un punto de inflexión. Por un lado, la arquitectura del sistema internacional se ve sujeta a una mayor presión y se recrudecen las controversias entre Estados. Por otro, se reivindica la necesidad de un multilateralismo eficaz para hacer frente a crisis de carácter global.

Se observa tensión entre las políticas de corte proteccionista o unilateral y los esfuerzos, sobre todo de la Unión Europea, para fortalecer el multilateralismo.

En los últimos años, las dinámicas de confrontación y competencia han prevalecido sobre las de negociación y acuerdo, lo que se ha traducido en un deterioro generalizado de las relaciones internacionales en todas sus facetas: comercial, tecnológica, diplomática o militar. Además, el declive democrático experimentado durante los últimos años contribuye a una mayor inestabilidad y dificulta la adopción de soluciones conjuntas.

En consecuencia, en muchas ocasiones, la gobernanza internacional en aspectos de seguridad, cambio climático o bienes públicos globales se ha visto suplantada por una cooperación ad hoc, marcada por alianzas de geometría variable. Esta tendencia se ha visto favorecida por los cambios en la distribución de poder y está contribuyendo a un multilateralismo de nuevo cuño, híbrido y con más actores emergentes y no estatales.

A su vez, ha aumentado el uso de las estrategias híbridas que, mediante acciones coordinadas y multidimensionales, tratan de explotar las vulnerabilidades de los Estados y sus instituciones con un objetivo de desestabilización o coerción política, social o económica. Estas estrategias se caracterizan por la dificultad de atribuir su autoría y por emplear medios que pueden incluir, además de acciones convencionales, otras como campañas de desinformación, ciberataques, espionaje, subversión social, sabotaje, coacción económica o el uso asimétrico de medios militares.

De forma destacada, la contestación del multilateralismo se enmarca en la creciente rivalidad geopolítica, comercial y tecnológica entre Estados Unidos y China. El esfuerzo de Estados Unidos por consolidar alianzas y retomar cierto liderazgo en la gobernanza global forma parte de este pulso entre ambas potencias.

La expansión económica de China, junto con un mayor proteccionismo de Estados Unidos, han provocado una creciente tensión en sus relaciones comerciales. Esta situación se ha materializado en una escalada de medidas arancelarias y restricciones a la exportación y la inversión adoptadas por ambas potencias.

La disputa es particularmente intensa en el ámbito tecnológico, donde se está produciendo una carrera por la supremacía mundial, que incluye el control de exportaciones

de tecnologías críticas y de doble uso. China, que ha logrado un gran desarrollo en la tecnología 5G y la Inteligencia Artificial busca alcanzar una posición de preeminencia que le permita definir los estándares y protocolos técnicos e industriales, así como ostentar el liderazgo en inversiones extranjeras directas en los operadores de redes y servicios.

Esta competición podría dar lugar a una brecha digital y productiva que desemboque en el desarrollo paralelo, pero diferenciado, de dos bloques tecnológicos. De esta forma, podría producirse un escenario de desacoplamiento en el que las cadenas de suministro de sectores estratégicos serían repatriadas o sometidas a un mayor control.

Adicionalmente, China ha redoblado sus esfuerzos por aumentar su peso en las organizaciones internacionales, con el objetivo de alcanzar una posición que le permita influir en las reformas de la gobernanza global. En términos globales, su capacidad de influencia relativa a la de Estados Unidos ha aumentado significativamente en las últimas tres décadas y ha logrado suplantar la influencia de países occidentales en muchas regiones, particularmente de África y del Sudeste Asiático.

En este panorama de tensión, Rusia se ha esforzado en los últimos años por lograr una posición de mayor liderazgo en la escena internacional, apostando por la multipolaridad, el reconocimiento a su «singularidad» y el reparto de áreas de influencia. La política expansionista de Rusia se ha visto reflejada en sus intervenciones en Siria y Libia y en su acercamiento a potencias con aspiraciones regionales como Turquía, India o Irán.

Al mismo tiempo, el orden nuclear heredado de la guerra fría se ha visto erosionado con el desmantelamiento de varios de los acuerdos de control de armas que limitaban la carrera armamentística entre Estados Unidos y Rusia, como el Tratado sobre Fuerzas Nucleares de Alcance Intermedio (INF). Sin embargo, Estados Unidos ha firmado un acuerdo con Rusia que renueva el Tratado de Reducción de Armas Estratégicas, conocido como New START. Además, ha indicado su interés en un retorno al Plan de Acción Integral Conjunto (PAIC) sobre el programa nuclear iraní, del que se retiró en 2018.

Potencias regionales, como Irán o Turquía, también han reforzado su influencia geopolítica en un contexto de fragmentación global y conflictos regionales, sobre todo en Oriente Medio y el Mediterráneo. Es posible que los conflictos en Palestina, Israel, Libia, Irak, Siria o Yemen continúen siendo escenarios de enfrentamiento entre diferentes actores estatales y no estatales, tanto nacionales como extranjeros.

La retirada de Estados Unidos y de la OTAN de Afganistán tras 20 años de presencia continua abre otro frente de competición geoestratégica, además de significar un posible uso del territorio afgano como refugio y base de acciones terroristas por parte de grupos yihadistas.

Por otro lado, la inestabilidad generada en el Mediterráneo oriental por las prospecciones gasísticas en el mar territorial en disputa entre Turquía, Chipre y Grecia muestra una tendencia a la unilateralidad en los litigios marítimos, dificulta una postura común de la Unión Europea y aumenta la dificultad de consenso dentro de la OTAN.

África subsahariana se está convirtiendo en escenario de rivalidades entre distintas potencias extrarregionales. En el Sahel, la desestabilización causada por el terrorismo yihadista se solapa con conflictos intercomunitarios en Estados que carecen de fortaleza institucional para hacer frente con éxito a este desafío múltiple. Todas estas dinámicas, unidas a la pobreza y desigualdad, agudizan la inseguridad imperante en varios países de la región.

Por su parte, la Unión Europea continúa su apuesta por una sólida relación transatlántica, al tiempo que define su postura hacia China entre la competición y la cooperación, en un ambiente de creciente inestabilidad en su vecindario oriental.

En este contexto multipolar y competitivo, se incrementa la necesidad de reforzar la autonomía estratégica de la Unión Europea, tanto en términos de política comercial e industrial comunitaria como en el desarrollo pleno de su Política Exterior y de Seguridad Común. Para ello, tendrá que lograr un equilibrio acorde con los compromisos de Derecho Internacional sobre la protección y garantía de los derechos humanos y con su papel como defensora de la democracia, el libre comercio y el multilateralismo.

*Escenario socio-económico*

La pandemia de la COVID-19 desencadenó la peor crisis económica mundial desde la Segunda Guerra Mundial, con una caída sin precedentes del Producto Interior Bruto (PIB) y de la actividad laboral mundial. La magnitud de sus efectos ha sido muy desigual, en función del tejido productivo de cada país, de los recursos económicos y de sus niveles de endeudamiento.

La repercusión de la crisis sobre la economía global en términos de PIB ha sido mayor que la de 2008, aunque ha estado seguida de un pronunciado repunte alcista. En un contexto de reducido crecimiento de la productividad en Europa y Estados Unidos, el impacto sobre las economías ha sido notable y podría acelerar el cambio en el equilibrio de poder de oeste a este. China es la única economía del G20 que no sufrió una recesión en 2020.

Si bien se espera que las consecuencias económicas negativas sean transitorias y que estén seguidas de tasas de crecimiento relativamente elevadas, se prevé un periodo de endeudamiento alto, fruto de las medidas extraordinarias de apoyo a ciudadanos y empresas adoptadas por la Unión Europea para hacer frente a la crisis.

En este sentido, la Unión Europea ha puesto en marcha un ambicioso Fondo de Recuperación y Resiliencia como respuesta común al proceso de transformación económica. El mecanismo Next Generation EU cuenta con 750.000 millones de euros financiados mediante la emisión de deuda comunitaria, que se suman a los 1.074 billones de euros del Marco Financiero Plurianual 2021-2027 para promover la recuperación económica y social y para favorecer un entorno de estabilidad y seguridad.

La crisis también ha puesto de relieve la dependencia del abastecimiento exterior de suministros estratégicos hay que añadir la puesta en marcha, por parte de los Estados, de políticas industriales estratégicas para hacer frente a la elevada competición global en determinados sectores tecnológicos e industriales.

La pugna económica y comercial entre las grandes potencias incluye el uso de los aranceles como instrumento de geopolítica, con su consiguiente impacto sobre las economías de la Unión Europea.

La súbita ralentización de la economía, el aumento de la desigualdad, la brecha digital, la destrucción de tejido productivo y el cierre de pequeñas y medianas empresas han derivado en un incremento de la pobreza y del nivel de frustración, marginalidad y exclusión social. Las clases medias, tras una década de crecimiento, se están contrayendo, mientras se expande la franja de población con ingresos bajos o muy altos. Este vaciamiento de las clases medias podría tener importantes consecuencias como el impacto negativo en el consumo global y el potencial incremento de populismos y autoritarismos identitarios, que podrían verse agravadas por los efectos de la automatización de los empleos. En este sentido, es preciso abordar un nuevo contrato social, para paliar la desigualdad y mitigar el proceso de precarización de las clases medias.

En algunos países, la crisis económica ha estado acompañada de una crisis social y política, alentada por campañas de desinformación y desestabilización que pretenden erosionar las instituciones, influir en los procesos democráticos y alentar la polarización.

Ante este escenario, la transformación digital y la transición ecológica cobran especial trascendencia como palancas de cambio de la estructura productiva de las economías mundiales y, en consecuencia, del mapa geopolítico. La digitalización y la economía verde habrán de avanzar de manera acompasada, de manera que la tecnología contribuya a alcanzar objetivos ecológicos y las tecnologías digitales minimicen su consumo energético y sus emisiones.

*Transformación digital*

El incremento de infraestructuras y servicios digitales, potenciado por tecnologías disruptivas y emergentes como la computación en la nube, la computación cuántica, la Inteligencia Artificial la virtualización de redes o el Internet de las Cosas, implica una transformación digital imparable que ofrece innumerables oportunidades de futuro, pero también presenta serios desafíos para la Seguridad Nacional.

En este contexto, la pandemia de la COVID-19 supuso una aceleración del proceso de digitalización, que ha situado a la interacción digital en el centro de las actividades públicas, privadas y profesionales y ha consolidado la hiperconectividad como rasgo definitorio redes y los sistemas de información y comunicaciones.

La digitalización de todo tipo de actividades ha ampliado la superficie de exposición a posibles ciberataques de organizaciones, tanto públicas como privadas, y ha dificultado la adecuada protección de la información. La magnitud y frecuencia de los ciberincidentes y del uso ilícito del ciberespacio han aumentado en los últimos años y han convertido la ciberseguridad en una prioridad de organizaciones y gobiernos.

Esta transformación digital no es un fenómeno solo tecnológico, sino que tiene impacto en las relaciones sociales y la configuración geopolítica. Los cambios tecnológicos generan cambios de poder, tanto dentro de los Estados como entre ellos. Con la consolidación del ciberespacio como dominio estratégico, se acentuará la brecha tecnológica tanto entre individuos y sociedades como entre países.

La estabilidad económica y las políticas monetarias también se ven afectadas por la irrupción de tecnologías potencialmente disruptivas. En particular, la configuración actual del sistema financiero global puede verse desafiada por la implantación de divisas digitales.

En este ámbito, los riesgos se ven amplificados por la prevalencia de criterios comerciales frente a los de seguridad en el diseño de productos de hardware y software, así como de sistemas y servicios, tales como el 5G. Este hecho dificultad los procesos de certificación y puede comprometer la cadena de suministro, especialmente en la provisión de servicios esenciales y/o críticos.

Otros riesgos, pero también múltiples oportunidades, derivan de los avances tecnológicos en campos como la biotecnología, que han facilitado el rápido desarrollo de vacunas eficaces contra la COVID-19, pero plantean interrogantes éticos ante actividades como determinados empleos de la ingeniería genética.

Por otro lado, la vulnerabilidad ante posibles injerencias de terceros es extensible al dominio de infraestructuras digitales, como los centros de procesamiento de datos o los cables submarinos, y a los activos que sustentan la propiedad intelectual e industrial del sector empresarial. También habrá que considerar el mapa mundial de conectividad y la aparición de nuevos operadores satelitales, especialmente aquellos vinculados a las grandes empresas tecnológicas.

Con el dato convertido ya en un recurso estratégico de primer orden, se ha intensificado el debate sobre la ética y la defensa de derechos digitales, condicionado especialmente por la concentración de la información en las grandes compañías tecnológicas y por su uso abusivo por parte de algunos actores políticos. En este debate, el derecho a la privacidad de los usuarios de servicios digitales ocupa un lugar central y ha dado lugar a pronunciamientos judiciales que podrían condicionar el desarrollo tecnológico.

El acceso seguro a los servicios públicos y privados, en particular a los servicios esenciales en línea, supone que la ciudadanía pueda proteger su identidad y controlar los datos que comparte y cómo se utilizan, de manera que se garantice la privacidad y la protección de datos personales. Disponer de una identidad digital segura es una pieza clave para la ciberseguridad.

La gobernanza democrática sobre el futuro digital es de máxima importancia para resolver las inquietudes relativas a los derechos y libertades y a la competición geopolítica.

*Transición ecológica*

La crisis climática ha dado paso a una mayor concienciación política y social de la necesidad de luchar contra sus consecuencias a través de procesos de transición ecológica.

El cambio climático tiene un impacto negativo en la vida y el bienestar humano. Entre sus efectos se encuentran el incremento en el número de fenómenos meteorológicos extremos, la degradación de ecosistemas terrestres y marinos, la desertificación, el aumento de la incidencia y frecuencia de olas de calor, las sequías, la reducción de las disponibilidades de agua, las intrusiones de polvo sahariano, los incendios forestales e inundaciones y la pérdida de la biodiversidad. Estos efectos perniciosos podrían llevar a una mayor competencia por los recursos y al incremento de desplazamientos migratorios desde zonas más expuestas a las consecuencias dañinas del cambio climático.

Por otro lado, la degradación de la biodiversidad produce la pérdida de sus servicios ecosistémicos, esenciales para el bienestar e incluso la supervivencia del ser humano, y propicia la expansión de especies exóticas invasoras, responsables de impactos relevantes en la economía y potenciales vectores de nuevas enfermedades.

En este contexto, la adaptación al cambio climático es básica para conseguir una resiliencia ambiental y ecológica que preserve la vida y el bienestar de la sociedad y el medio.

En diciembre de 2019, la Unión Europea presentó el Pacto Verde Europeo, una hoja de ruta para hacer que su economía sea sostenible y neutral climáticamente en 2050. Para ello, se ha establecido el objetivo vinculante de conseguir, en 2030, una reducción interna neta de emisiones del 55% respecto a los niveles de 1990. En este marco, es igualmente importante el impulso hacia una economía circular con un modelo de producción y consumo basado en reutilizar, renovar y reciclar materiales y productos. Este modelo ayudará a reducir la presión sobre el medio ambiente, a mejorar la seguridad de las cadenas de suministro mediante un empleo más efectivo de los recursos existentes y a estimular el desarrollo empresarial en el campo de la I+D+i.

Un aspecto clave para lograr la neutralidad climática es el cambio del paradigma energético, que transita de la dependencia de los combustibles fósiles a la de las tecnologías renovables. Esto propiciará una nueva geopolítica de transición energética y un cambio en el equilibrio entre importadores y exportadores.

El desarrollo de energías renovables tiene además un carácter estratégico, ya que permitirá el uso de fuentes autóctonas y una mayor diversificación, lo que incrementa la seguridad y mejora la balanza exterior. Sin embargo, también conlleva importantes desafíos tecnológicos relacionados con un sistema de generación eléctrica basado en fuentes de energía variable, el desarrollo de nuevos sistemas de almacenamiento e infraestructuras inteligentes, así como retos relacionados con la reducción del impacto sobre el medio natural y humano.

La evolución hacia una economía descarbonizada incrementará la competencia por las materias primas, como las tierras raras, los materiales y procesos industriales relacionados con la digitalización y las tecnologías renovables, así como una mayor dependencia de las regiones geográficas abastecedoras de estas tecnologías.

## CAPÍTULO 2

### Una España segura y resiliente

El segundo capítulo de la Estrategia de Seguridad Nacional ofrece un recorrido de las distintas regiones geográficas del mundo desde la perspectiva española de la seguridad.

España es un Estado social y democrático de Derecho, dotado de un marco constitucional de derechos y libertades que tiene al ciudadano como eje central, con unas instituciones sólidas y plenamente democráticas. Una de sus principales fortalezas reside en su sociedad plural, abierta y solidaria.

La visión de futuro de una España segura y resiliente incluye la transformación tecnológica y la transición ecológica como vectores que faciliten un crecimiento sostenible y justo, la competitividad del tejido industrial y empresarial y la creación de empleo de calidad.

La Seguridad Nacional debe contribuir a la cohesión territorial y es necesario asegurar que todas sus estructuras sean más resilientes frente a los riesgos y las amenazas.

Desde una perspectiva geográfica, la configuración de España es singular, con una dimensión territorial peninsular, archipiélagos, islas, peñones y las Ciudades Autónomas de Ceuta y Melilla en el norte de África, además de una significativa extensión marítima.

Su posición le confiere la condición de país europeo, mediterráneo y atlántico que se proyecta al mundo como un contribuyente comprometido con la paz y la seguridad internacional. España defiende el refuerzo del multilateralismo, la profundización en la construcción europea, las alianzas bilaterales estratégicas y el compromiso solidario como principios establecidos en la Estrategia de Acción Exterior. La cooperación con los vecinos fronterizos, Francia, Andorra, Portugal y Marruecos es especialmente relevante.

La Estrategia de Seguridad Nacional está alineada con los objetivos de las organizaciones a las que España pertenece, especialmente las Naciones Unidas, la Unión

Europea y la OTAN, con las que pretende proteger y garantizar los intereses compartidos con sus socios y aliados.

*Europa*

España es un Estado miembro con peso dentro de la Unión Europea, firme defensor del avance en la construcción europea y proactivo en el desarrollo de políticas comunes en áreas de especial relevancia como la energía, la inmigración y la seguridad.

Para España, una Unión más resiliente es una Europa más fuerte en el mundo. La Unión Europea debe seguir avanzando en el desarrollo de su Política Exterior y de Seguridad Común, en especial de su Política Común de Seguridad y Defensa, frente a desafíos derivados del empleo de estrategias híbridas y de posturas adversas de actores como Rusia y China o de fenómenos como el terrorismo, así como en la coordinación y cooperación con la OTAN y las Naciones Unidas.

La protección de los espacios y rutas marítimas es clave para la seguridad europea. El margen atlántico es un área de interés estratégico que conecta Europa con todo el continente americano y con África occidental. El progresivo deshielo del Ártico abre nuevas rutas marítimas con implicaciones estratégicas. Además, España comparte agenda en áreas como el golfo de Guinea, con otros países europeos atlánticos, como es el caso de Francia y Portugal, principalmente en relación con la seguridad marítima y energética.

Al sur de Europa, el mar Mediterráneo es un nexo común y un puente estratégico con África y Oriente Medio, pero también un escenario de tensión y fricción donde distintos países y actores pretenden imponer su criterio y sus intereses, en ocasiones de espaldas al Derecho Internacional y violando la soberanía de los Estados ribereños.

En este sentido, España trabajará para promover el diálogo en torno al Mediterráneo oriental, de acuerdo con la perspectiva de la Unión Europea y en el entendimiento de que Turquía es un actor regional clave, un aliado en la OTAN y un socio estratégico con intereses compartidos.

En el flanco oriental, la posición cada vez más asertiva de Rusia ha tensionado sus relaciones con la Unión Europea, que además ha constatado el desafío que suponen algunas de las acciones procedentes de ese país, tanto militares como híbridas. España seguirá apostando por mantener el diálogo con Rusia, a pesar de las dificultades, sobre la premisa del respeto al Derecho Internacional, la defensa de la soberanía y la integridad territorial de los Estados y el respeto a los derechos humanos en su acción exterior.

La salida de Reino Unido de la Unión Europea ha modificado el escenario europeo y presenta retos relacionados con la pérdida de un gran activo en el ámbito de la seguridad. Para España, esta salida no impedirá fortalecer los vínculos entre dos países amigos y aliados. No obstante, y desde la base de una cooperación positiva, España no renuncia a la oportunidad que se abre con este nuevo escenario para solventar el anacronismo que representa la situación de Gibraltar.

*Magreb y Oriente Próximo*

La prioridad de España en el Magreb es promover un espacio de seguridad, estabilidad política y desarrollo y contribuir a enfrentar amenazas, como el terrorismo o el crimen organizado, desde un enfoque de colaboración con países que son socios y amigos preferentes de España.

La relación de España con Marruecos y Argelia es de buena amistad, desde la premisa de la cooperación leal y el respeto a las fronteras mutuas. La colaboración con estos países en aspectos relacionados con la seguridad, como los tráficos ilegales o el terrorismo, complementa unas sólidas relaciones basadas en el diálogo político, las relaciones comerciales y los vínculos energéticos.

El apoyo a la convulsa democracia en Túnez y la contribución a los esfuerzos liderados por las Naciones Unidas para solventar la crispada situación que atraviesa Libia son también imprescindibles para lograr la paz y la estabilidad en el Mediterráneo.

La región de Oriente Próximo es un foco de atención internacional por su persistente inestabilidad, pero también por la proliferación de conflictos internos, la extensión del terrorismo yihadista, las graves crisis humanitarias y la injerencia de determinados actores

globales y regionales al margen de marcos multilaterales. La guerra en Siria y Yemen y la tensión entre Irán y las monarquías del Golfo dibujan un panorama complejo. Por otro lado, el repliegue de Estados Unidos de determinados escenarios de Oriente Próximo dejará un vacío que será aprovechado por actores como Rusia y China. Enfrentar todos estos desafíos exige una firme y amplia cooperación internacional.

España es un país comprometido con la seguridad de la región, con militares desplegados tanto en el Líbano, en el marco de las Naciones Unidas, como en operaciones de la OTAN, la Unión Europea y la Coalición Global contra el Daesh.

España ha apoyado de manera activa, desde la conferencia de Paz de Madrid en 1991, una solución al conflicto palestino-israelí a través del Proceso de Paz en Oriente Próximo. Los acuerdos entre Israel y Emiratos Árabes Unidos, Bahréin y Marruecos en 2020 muestran la rapidez y profundidad de los cambios en la región, así como la necesidad de adaptar la posición española para que siga siendo útil en la búsqueda de una solución justa con ambas partes.

*África Subsahariana*

El nexo seguridad-desarrollo y un enfoque preventivo son los principios que guían las políticas para la contribución de España a la estabilidad en tres áreas geográficas de especial interés: el Sahel, el golfo de Guinea y el Cuerno de África, tal y como se recoge tanto en el III Plan África como en el programa Foco África 2023.

España mantendrá el apoyo a las iniciativas de seguridad internacionales y regionales, así como su compromiso con las misiones civiles y militares de la Unión Europea en África.

En el Sahel, la permanente crisis de gobernabilidad y la ausencia del Estado en grandes espacios de soberanía se suman a emergencias humanitarias por desastres naturales o por los efectos adversos del cambio climático. Todo ello en un entorno de fragilidades estructurales que, unidas a la presión sobre los limitados recursos para una población caracterizada por su elevado crecimiento demográfico, han exacerbado amenazas latentes como son el terrorismo yihadista, los numerosos conflictos intercomunitarios o los tráficos ilícitos. Además, los factores de inestabilidad del Sahel, y en particular la amenaza del extremismo violento, se extienden hacia los países costeros de África occidental y norte de África.

Los países del golfo de Guinea tienen una gran importancia estratégica para Europa y para la salvaguardia de los intereses españoles. En sus espacios marítimos proliferan actividades delictivas como los secuestros y el robo a mano armada en los buques pesqueros y petroleros, o la piratería y la pesca ilegal en aguas internacionales. En el golfo de Guinea, España contribuye activamente a una navegación segura en las rutas y espacios marítimos, con el objetivo de fortalecer la seguridad marítima nacional y regional a fin de garantizar también el suministro energético, la protección de la pesca y las inversiones españolas en la región.

En el Cuerno de África, la aplicación de un enfoque integral que aborde las raíces de los conflictos que afectan a rutas y espacios marítimos de alta importancia internacional seguirá orientando la acción de España. Además, España sigue con preocupación los acontecimientos en el norte de Mozambique, que representan un foco de inestabilidad para la región en su conjunto.

*América del Norte y el Vínculo Transatlántico*

La alianza estratégica de España con Estados Unidos está basada en una relación de mutua confianza a con dimensiones políticas, económicas, culturales y militares. El Convenio de Cooperación para la Defensa, suscrito entre ambos países, constituye un valor añadido, sin olvidar tampoco la buena colaboración, junto a otros socios y aliados, en el seno de la Coalición Global contra el Daesh.

El escenario actual abre una ventana de oportunidad para la consolidación del vínculo transatlántico y el refuerzo y reforma del multilateralismo y sus instituciones. También se ha de tener en consideración el giro estratégico de Estados Unidos hacia el Indo-Pacífico y su presencia más reducida en Oriente Medio. España, miembro de la Unión Europea y de la

OTAN, apoyará la cooperación entre las dos organizaciones como eje central de la seguridad colectiva frente a los grandes desafíos globales.

*América Latina y el Caribe*

América Latina ha experimentado un rápido desarrollo en la primera década del siglo XXI. Sin embargo, enfrenta aún importantes desafíos, que se han agudizado por efecto de la pandemia de la COVID-19: inseguridad ciudadana, crisis medioambientales y desastres naturales, altos índices de corrupción, tráficos ilícitos y crimen organizado.

España fomentará la unión y la estabilidad en América Latina a través de la acción bilateral, los foros regionales y las Cumbres Iberoamericanas. Además, redoblará sus esfuerzos para servir de puente de entendimiento y colaboración con la Unión Europea y fomentar la colaboración en la gestión de crisis que afectan a todos.

España seguirá colaborando con la erradicación de la producción y el tráfico de drogas desde América Latina, por la amenaza que supone para la región y por ser España uno de los puntos de entrada a Europa de estos tráficos ilícitos.

España también se esforzará en mantener su privilegiada relación con América Latina sobre la base de una cooperación reforzada y una relación más estrecha en el ámbito de la Defensa, especialmente a través de la cooperación en operaciones de apoyo a la paz, en el nivel bilateral y regional.

*Asia-Pacífico*

El progresivo desplazamiento del centro de gravedad económico y estratégico mundial hacia el área de Asia-Pacífico hace que sea una zona de interés para España.

La Unión Europea ha señalado su compromiso con la estabilidad y prosperidad en la región del Indo-pacífico, un área geográfica clave para la seguridad internacional que está experimentando una creciente competición geopolítica.

Los litigios marítimos en el mar del sur de China, las tensiones en torno a Taiwán, el conflicto sobre Cachemira o las disputas fronterizas entre India y China introducen elementos de inestabilidad regional, que se suman a amenazas como el desarrollo de armas y vectores nucleares en la República Popular Democrática de Corea o la expansión del terrorismo transnacional de carácter yihadista.

Países como India y China ocupan cada vez mayor espacio en los asuntos internacionales. Por otro lado, iniciativas regionales como el Acuerdo de Asociación Económica Integral Regional amplifican la influencia de la región en la economía mundial.

El ascenso de China como potencia global se proyecta a través de su nueva ruta de la seda, su dominio tecnológico y una creciente presencia inversora en América Latina y África, así como en países europeos. En su relación con Pekín, la Unión Europea combina elementos de rivalidad sistémica, áreas de competición y retos globales comunes, como el cambio climático o la no proliferación de armas nucleares, que requieren cooperación.

La situación en Afganistán tras la retirada de Estados Unidos podría tener un impacto geopolítico significativo con la posible reconfiguración de las relaciones tanto a nivel global como regional. El potencial deterioro de la situación humanitaria y de derechos humanos presenta un desafío adicional. Además, para la seguridad de Europa será especialmente importante evitar que el país vuelva a convertirse en un santuario para terroristas y un foco de crimen organizado.

España apoya las iniciativas de refuerzo de la cooperación en la región en áreas como la conectividad y la seguridad marítima, así como la acción concertada frente a desafíos de dimensión global, como el cambio climático y la salud, y el impulso de las relaciones comerciales. Además, profundizará las relaciones con aquellos países de la región con los que comparte valores e intereses.

## CAPÍTULO 3

## Riesgos y amenazas

El tercer capítulo de la Estrategia de Seguridad Nacional describe un mapa de los riesgos y amenazas a la Seguridad Nacional con un enfoque que pone de relieve su

dinamismo e interdependencia, en un entorno de seguridad donde las estrategias híbridas ganan protagonismo.

El panorama actual de seguridad es más incierto que en años anteriores. La crisis de la COVID-19 ha intensificado las tendencias globales de fondo y ha acelerado el ritmo de transformación.

La superficie de confrontación geopolítica encuentra áreas de intersección con la tecnología y la economía, dibujando así un mapa de riesgos más complejos y muy interrelacionados. Adicionalmente, amenazas derivadas del uso de tecnologías de nueva generación, como la Inteligencia Artificial o el acceso al espacio ultraterrestre, añaden complejidad y dificultan la protección de los derechos individuales ante un eventual uso malicioso.

En esta Estrategia, los factores que afectan a la Seguridad Nacional se plantean como elementos de un continuo que refleja una gradación progresiva en función de su grado de probabilidad e impacto. Así, los riesgos y las amenazas no son estáticos, sino que se conciben de una manera dinámica.

Además, se presenta un mapa de riesgos con dos características diferenciales con respecto a modelos anteriores. Por un lado, se subraya el papel primordial de la tecnología en la mayoría de las amenazas y la prominencia de las estrategias híbridas y, por otro, se acentúan las interconexiones entre los distintos riesgos y amenazas. De esta forma, la interrelación entre ellos puede producir efectos en cascada, como ha ocurrido con la crisis generada por la pandemia.

Con este planteamiento, es importante contar con las capacidades necesarias para responder a una amalgama de riesgos y amenazas, en lugar de prepararse solamente para una posible repetición de una crisis similar a la ya experimentada.

*Tensión estratégica y regional*

En el contexto de seguridad actual, caracterizado por un retroceso del multilateralismo, un aumento de la asertividad de ciertos actores y un incremento de la competición estratégica entre Estados, el riesgo de que se produzcan tensiones con impacto directo sobre los intereses nacionales e incluso sobre la propia soberanía, constituye una seria amenaza para la Seguridad Nacional, cuya máxima expresión podría llegar a adoptar la forma de conflicto armado.

Esta situación se ve agravada por la fragilidad y vacíos institucionales en algunas regiones próximas, cuyos conflictos internos pueden, igualmente, afectar a los intereses de España. Estos escenarios de inestabilidad, si no son contenidos a tiempo, pueden tensionar aún más las relaciones internacionales, elevando el riesgo de conflictos entre Estados a nivel regional.

En este clima de creciente tensión internacional, donde determinados actores se rearman para fortalecer sus aspiraciones estratégicas, España requiere una capacidad de disuasión creíble y efectiva y una capacidad de defensa autónoma, frente a diferentes formas de agresión: desde las estrategias híbridas hasta el conflicto convencional. España debe, además, seguir siendo un socio comprometido y fiable de la Unión Europea, la OTAN, las Naciones Unidas y otros marcos multinacionales de seguridad y defensa.

En este contexto y debido a la naturaleza cambiante de los conflictos, los tradicionales dominios terrestre, naval y aéreo, se ven ahora complementados por la aparición de nuevos espacios de competición, como el ciberespacio y el espacio ultraterrestre, que obligan a incorporar nuevas formas de actuación, así como tecnologías de última generación para mantener una capacidad de enfrentamiento actualizada y moderna.

*Terrorismo y radicalización violenta*

La polarización y la crisis económica han contribuido a un incremento en la actividad de los extremismos violentos.

Los medios utilizados por los grupos terroristas son cada vez más variados y los ataques físicos están acompañados de campañas propagandísticas que alimentan ideologías radicales violentas.

En esta amenaza cobra especial relevancia el terrorismo yihadista, con su presencia tanto en distintos países europeos, como en el Sahel, Magreb y Oriente Medio, desde donde se proyecta la amenaza terrorista sobre España. Existe además el riesgo de ataque sobre individuos e intereses nacionales en estas regiones.

Dentro de las fronteras de España, la principal amenaza proviene de individuos que han nacido o crecido en países occidentales que, tras ser radicalizados, atacan en su propia área de residencia. Igualmente relevante es la amenaza derivada de los procesos de radicalización en prisiones.

Además, el posible retorno de personas desplazadas a zonas de conflicto para apoyar a los grupos terroristas constituye un riesgo significativo. Por ello, es necesario fortalecer la cooperación y colaboración en materia antiterrorista y judicial, no solo entre los Estados miembros de la Unión Europea, sino también con terceros países, bajo un enfoque multidisciplinar.

*Epidemias y pandemias*

La crisis desencadenada por la COVID-19, además de cobrarse la vida de millones de personas en el mundo, ha tenido importantes consecuencias sociales y económicas, con un impacto desigual que ha agudizado las brechas existentes entre países, sociedades y ciudadanos.

Las dificultades experimentadas por los organismos internacionales para la toma de decisiones y las tensiones surgidas en relación con la producción y distribución de material sanitario, fármacos o vacunas dirigidos a combatir la enfermedad han contribuido a intensificar fricciones geopolíticas existentes y, en determinados casos, a dificultar la cooperación internacional.

Un aspecto crucial que se ha puesto de manifiesto es la fragilidad de las cadenas de suministro global de determinados recursos estratégicos y la necesidad de disminuir el grado de dependencia del exterior de recursos esenciales para garantizar su accesibilidad en todo momento.

*Amenazas a las infraestructuras críticas*

Las Infraestructuras Críticas posibilitan el normal desarrollo de la actividad socio-económica y son objetivo de amenazas, tanto físicas como digitales, que podrían llevar a una interrupción o negación de servicios.

La progresiva digitalización y la adopción de nuevas tecnologías por parte de los operadores críticos y operadores de servicios esenciales podría aumentar el riesgo de sufrir brechas de seguridad, que permitirían acceder al control de los sistemas que operan las Infraestructuras Críticas y poner en peligro la continuidad de los servicios que proveen.

Otro riesgo a considerar es la potencial pérdida de control sobre la capacidad de decisión estratégica a raíz de inversiones por actores, estatales o no estatales, con intereses no necesariamente alineados con la Seguridad Nacional.

*Emergencias y catástrofes*

La seguridad de las personas y los bienes se ve afectada por distintos tipos de emergencias y catástrofes originadas por causas naturales o derivadas de la acción humana accidental o intencionada.

Factores potenciadores del riesgo de emergencias y catástrofes son tanto la despoblación rural como la sobrepoblación de algunas ciudades, la degradación del ecosistema agravada por los efectos del cambio climático o el incremento en la magnitud y frecuencia de algunos fenómenos meteorológicos adversos.

En este contexto, se identifican como principales riesgos las inundaciones, los incendios forestales, los terremotos y maremotos, los riesgos volcánicos, los fenómenos meteorológicos adversos, los accidentes en instalaciones o durante procesos en los que se utilicen o almacenen sustancias peligrosas, el transporte de mercancías peligrosas por carretera y ferrocarril, los accidentes catastróficos en el marco del transporte de viajeros y los riesgos nucleares, radiológicos y biológicos.

*Espionaje e injerencias desde el exterior*

El incremento de la competitividad y de la tensión en el escenario internacional ha supuesto un aumento de las injerencias desde el exterior que España debe confrontar. Entre las herramientas más eficaces de algunos países que aspiran a expandir su influencia internacional destacan las actividades de espionaje.

La pertenencia de España a organizaciones como la Unión Europea y la OTAN, hacen del país un objetivo atractivo. Sin embargo, los objetivos de los Servicios de Inteligencia hostiles no se limitan a las instituciones y a la información del Gobierno de España, también afectan a otros sectores, como por ejemplo a la industria de defensa, las Infraestructuras Críticas o la investigación científica y tecnológica, así como a otros ámbitos del sector privado. Estas actividades no solo son críticas para la Seguridad Nacional, sino que pueden atentar contra la competitividad económica y la propiedad intelectual, especialmente en lo que respecta a los sectores estratégicos y al campo de la ciencia y la investigación.

Asimismo, son destacables los esfuerzos de algunos actores extranjeros por influir sobre sus nacionales asentados en España, afectando a los derechos y libertades de los ciudadanos y, potencialmente, a la estabilidad social.

En otras ocasiones, las actuaciones de los Servicios de Inteligencia extranjeros no tienen como objetivo intereses españoles o aliados, sino que utilizan el territorio español como base de sus operaciones en otros países, pudiendo atentar contra la soberanía nacional.

Tanto las actividades de inteligencia clásicas como el ciberespionaje son una importante amenaza en sí mismos. Pero, además, hay que considerar que las actividades de los Servicios de Inteligencia hostiles pueden formar parte de las llamadas estrategias híbridas. Dentro de estas estrategias, las actividades de espionaje pueden llegar a ser un elemento destacable y potencian la amenaza que suponen para la Seguridad Nacional.

*Campañas de desinformación*

Las campañas de desinformación tienen clara repercusión en la Seguridad Nacional y deben diferenciarse de otros factores como la información falsa –*fake news*– o información errónea –*misinformation*–. De hecho, las campañas de desinformación no contienen necesariamente noticias falsas, sino que pretenden distorsionar la realidad mediante contenido manipulado.

En este sentido, el ámbito cognitivo es un espacio más en el que ejercer influencia, que se suma a los tradicionales ámbitos físicos: terrestre, marítimo y aéreo. Los elementos que sí son inherentes a una campaña de desinformación son la voluntad de generar confusión y socavar la cohesión social; el uso coordinado de distintos medios para la creación y difusión de contenidos dirigidos a audiencias amplias; y la intención maliciosa con fines de desprestigio o influencia sobre el objetivo del ataque. Así, las campañas de desinformación suponen una grave amenaza para los procesos electorales.

Por su potencial peligrosidad, cabe señalar las estrategias de desinformación de actores extranjeros, tanto estatales como no estales, que desarrollan aparatos de propaganda con la intención de polarizar a la sociedad y minar su confianza en las instituciones.

*Vulnerabilidad del ciberespacio*

Se distinguen dos tipologías generales de amenazas en el ciberespacio. Por un lado, los ciberataques, entendidos como acciones disruptivas que actúan contra sistemas y elementos tecnológicos. Ejemplos de ello son los ataques de *ransomware* (secuestro de datos) o la denegación de servicios, entre otros. Y, por otro lado, el uso del ciberespacio para realizar actividades ilícitas, como el cibercrimen, el ciberespionaje, la financiación del terrorismo o el fomento de la radicalización.

La creciente exposición digital amplía la superficie de exposición a ciberataques de ciudadanos, empresas y administraciones. Entre las dinámicas que marcan un mayor revolución industrial, el despliegue de las redes 5G multiplicará la capilaridad de las redes y con ello aumentará de manera significativa su uso, no solo por usuarios sino en el segmento Internet de las Cosas y las comunicaciones máquina-a-máquina. Consecuentemente, se generará un aumento de la vulnerabilidad ante ciberataques en aparatos conectados a la red y servicios como el vehículo autónomo o las redes inteligentes.

Asimismo, en la denominada sociedad virtual, el dato constituye un nuevo ámbito de poder que afecta tanto a la relación entre Estados como entre el sector público y el privado, al ser las compañías tecnológicas las que poseen un mayor acceso a los datos. La seguridad de la información afecta al ciudadano de forma directa. La regulación, protección y garantía del uso adecuado de los datos y las redes por las que transitan es un aspecto clave de la Seguridad Nacional, con impacto directo sobre la privacidad personal.

Tecnologías como la Inteligencia Artificial y el *big data* subyacen cada vez más en ámbitos como el sanitario, el de transportes, el energético, el empresarial, el financiero, el educativo y el militar. La capacidad de procesamiento de grandes cantidades de datos se presenta como una característica avanzada para la consecución de los objetivos deseados. Su potencial de transformación y aplicación en procesos de análisis de riesgos y de alerta temprana es cada vez mayor. Pero el desarrollo de estas tecnologías también genera interrogantes relacionados con la seguridad. La aplicación de algoritmos para la toma automática de decisiones requiere un marco de protección de la privacidad y la no-discriminación. El empleo de sistemas autónomos también tiene implicaciones éticas que requieren mecanismos de control y parámetros que garanticen el respeto a los derechos humanos.

En el medio-largo plazo, el salto tecnológico que supone la computación cuántica permitirá usos difíciles de prever hoy en día en materia de comunicaciones seguras, cifrado y descifrado y sistemas de vigilancia avanzados, entre otros.

*Vulnerabilidad del espacio marítimo*

El espacio marítimo es considerado uno de los espacios comunes globales, espacios de conectividad de flujos, información, personas, servicios y bienes, cuya interrupción u obstaculización puede tener un impacto económico severo.

Para España, país de condición marítima, es esencial mantener la seguridad en los espacios marítimos, así como asegurar el funcionamiento de las Infraestructuras Críticas situadas en el litoral y en el mar, como los puertos y tuberías submarinas y, especialmente, los cables submarinos, por los que circula la práctica totalidad del tráfico de datos. De su buen uso y estado depende, en gran medida, la economía, ya que los recursos energéticos y la mayor parte del comercio español transita por rutas marítimas.

La piratería y el robo a mano armada en la mar atentan contra la navegación segura por las principales rutas de tráfico marítimo y contra la flota pesquera de pabellón nacional, principalmente en la cuenca somalí, el golfo de Adén y el golfo de Guinea.

Además, los tráficos ilícitos, la explotación ilegal de los recursos marinos y los actos contra el patrimonio arqueológico subacuático son fenómenos perjudiciales para el sector marítimo.

*Vulnerabilidad aeroespacial*

El sector aeronáutico es de alta importancia estratégica. Cualquier disrupción que afecte a las aeronaves, los aeropuertos o las instalaciones en tierra, en especial un ataque terrorista, tendría un impacto de magnitud y trascendencia económica considerables.

La alta conectividad aérea entre países y continentes es, asimismo, una de las causas de la rápida propagación de enfermedades infecciosas a nivel internacional.

Una de las tendencias preocupantes es la proliferación del uso ilícito de vehículos aéreos no tripulados, que pueden paralizar el uso de aeropuertos o infraestructuras críticas, y son además potenciales armas para sabotajes o acciones terroristas.

El espacio ultraterrestre está considerado como la última frontera de confrontación geopolítica. Este espacio común global se ha convertido en un dominio de explotación comercial intensiva, con la proliferación de constelaciones de satélites y lanzadores comerciales. Sin embargo, algunos operadores, no radicados en la Unión Europea, están en el camino de alcanzar una posición de dominancia tal de los mercados que podría poner en riesgo tanto el acceso al espacio (lanzamientos) como a determinados servicios espaciales. En este sentido, las nuevas constelaciones de satélites pueden hacer insostenible el modelo de cooperación público-privada español en comunicaciones gubernamentales y observación de la Tierra.

Además, la falta de normativa legal facilita la actividad irregular en el espacio ultraterrestre y dificulta la protección de activos estratégicos, como las comunicaciones vía satélite, los sistemas de posicionamiento y tiempo o los satélites de observación terrestre. Por otro lado, la seguridad de los sistemas espaciales se verá seriamente afectada por el incremento de los desechos espaciales y la carencia de un sistema de gestión del tráfico espacial global.

*Inestabilidad económica y financiera*

La pandemia de la COVID-19 ha generado el mayor desplome del Producto Interior Bruto desde la Segunda Guerra Mundial, lo que ha causado una nueva crisis económica con consecuencias aún inciertas en clave social. Aunque el impacto económico sea fundamentalmente transitorio y esté seguido de tasas de crecimiento relativamente elevadas, ha causado un aumento de la situación de inestabilidad y desigualdad económica.

Entre los factores que pueden contribuir a la inestabilidad económica y financiera se incluyen los desequilibrios en las vías de financiación de la Hacienda Pública; la inestabilidad financiera internacional; el fraude, la evasión y la planificación fiscal; la corrupción; el blanqueo de capitales y el uso indebido de los fondos procedentes de subvenciones y contratos públicos. Estos factores socavan la seguridad económica y provocan desafección social de las instituciones gubernamentales.

*Crimen organizado y delincuencia grave*

El crimen organizado es una amenaza a la seguridad que se caracteriza por su finalidad esencialmente económica, su efecto horadador sobre la instituciones políticas y sociales, su carácter transnacional y su opacidad.

Los grupos delictivos y las organizaciones criminales camuflan sus operaciones ilegales con negocios lícitos y se apoyan cada vez más en tecnologías digitales, como las cripto-monedas y la Internet oscura.

Además de su dimensión económica, el crimen organizado tiene un relevante potencial desestabilizador. Sus estructuras se adaptan al entorno geoestratégico y repercuten en la gobernanza, la paz social y el normal funcionamiento de las instituciones.

En cuanto a la delincuencia grave, actividades como la explotación de menores o la trata con fines de explotación sexual se dirigen hacia los colectivos vulnerables y violan gravemente los derechos humanos. El contrabando, el cibercrimen, el tráfico de drogas, de armas y de especies silvestres y la corrupción son amenazas tangibles para la Seguridad Nacional.

La convergencia entre grupos terroristas y redes de crimen organizado va en aumento. Los modelos de organización cada vez más descentralizada de estos actores delictivos favorecen su cooperación y facilitan la financiación terrorista.

*Flujos migratorios irregulares*

El fenómeno de la migración contemporánea –global, complejo y multidimensional– tiende a difuminar las distinciones tradicionales entre países de origen, destino y tránsito. Los factores económicos, sociales y medioambientales, así como la inestabilidad política, la pobreza y los conflictos, seguirán influyendo en las tendencias migratorias mundiales. Asimismo, la multiplicación de las opciones de comunicación y desplazamiento favorecen una nueva era de movilidad humana. Junto a oportunidades, los movimientos migratorios seguirán generando retos –incluidos los de carácter securitario en sentido amplio– que hay que gestionar.

El desarrollo tanto en los países de origen como en los receptores de migrantes, se ve quebrado por las actividades ilícitas de organizaciones criminales dedicadas al tráfico y la trata de personas, que proliferan en torno a los movimientos migratorios y cuyas actividades conllevan graves vulneraciones de derechos humanos.

España, por su posición geoestratégica, está especialmente expuesta al desafío que supone el esperado aumento de los flujos migratorios hacia Europa en los próximos años. En su condición de frontera exterior de la Unión Europea, España afronta la gestión de los

flujos migratorios irregulares como un importante reto que requiere una política migratoria común, basada en el justo equilibrio entre solidaridad y responsabilidad compartida entre Estados. Los riesgos derivados de la inmigración irregular afectan directamente a la continuidad del espacio Schengen.

*Vulnerabilidad energética*

El proceso de transformación del sector energético lleva aparejado nuevos riesgos asociados a un modelo de generación verde. La disponibilidad de nuevas materias primas, las nuevas tecnologías de almacenamiento o la generación distribuida basada en energías renovables, el autoconsumo y la eficiencia son todos elementos a tener en cuenta en la ecuación energética actual.

La incorporación de medidas orientadas a garantizar la cohesión económica y territorial para paliar los efectos socioeconómicos de los cambios en las fuentes de energía primaria, como la transición justa, forman parte de la nueva visión de la seguridad energética en esta estrategia.

Si bien la dependencia de hidrocarburos provenientes del exterior seguirá siendo un factor de vulnerabilidad en los próximos años, la transición hacia un nuevo modelo energético económicamente sostenible y respetuoso con el medioambiente es el principal desafío de un sector clave para la economía y la seguridad, donde el cambio climático es considerado como un riesgo sistémico a nivel global.

*Proliferación de armas de destrucción masiva*

La modernización y el aumento del arsenal nuclear de China, India y Pakistán, junto con los avances del programa nuclear de la República Popular Democrática de Corea y el programa de enriquecimiento de uranio en Irán, contribuyen a diseñar un orden nuclear cada vez más multipolar. Este escenario podría desencadenar una nueva carrera armamentística definida por la posible reanudación de pruebas nucleares y el desarrollo de nuevas armas. A esto se suma la precariedad de los tratados vigentes para el control de la proliferación de armas de destrucción masiva y de sus vectores de lanzamiento.

La amenaza biológica, entendida como el empleo deliberado de agentes patógenos, toxinas o elementos genéticos u organismos genéticamente modificados dañinos por parte de Estados, individuos, redes criminales u organizaciones terroristas, supone una amenaza real con posibles consecuencias catastróficas.

El régimen de prohibición de armas químicas también se enfrenta a importantes retos, como los ataques registrados en los últimos años en Siria.

Asimismo, los riesgos derivados del desvío y contrabando de materiales de doble uso aumentan considerablemente debido a la transferencia de conocimiento tecnológico y el movimiento global de mercancías.

*Efectos del cambio climático y de la degradación del medio natural*

El cambio climático es una amenaza para la seguridad global y, en Europa, especialmente para el área mediterránea. Por eso la mitigación y adaptación al cambio climático adquieren cada vez más urgencia.

El cambio climático potencia las olas de calor, la reducción de los recursos hídricos, la desertificación y los fenómenos meteorológicos adversos. Ámbitos como la seguridad energética y la seguridad ambiental, en particular la gestión del agua, la biodiversidad, la calidad del aire, la despoblación de zonas agrarias o forestales se ven afectados por los efectos del cambio climático. Riesgos de origen natural relacionados con el clima, como son las inundaciones y los incendios forestales, tienen cada vez mayor incidencia en la seguridad, pues cada vez son más severos y frecuentes.

El deterioro del medio ambiente, de la biodiversidad y de sus servicios ecosistémicos dificultan el acceso a recursos básicos como el agua potable, amplifican conflictos existentes y son causa de desplazamientos forzosos de personas, además de generar inseguridad alimentaria.

CAPÍTULO 4

**Un planeamiento estratégico integrado**

Este capítulo establece los objetivos de la Estrategia y desarrolla un planeamiento integrado para la Política de Seguridad Nacional con una estructura diseñada con tres ejes estratégicos: Proteger, Promover y Participar.

La Estrategia de Seguridad Nacional establece tres objetivos:

El primer objetivo es avanzar en el modelo de gestión de crisis. Esto supone adoptar un enfoque anticipatorio y centrar la toma de decisiones en el análisis de hechos y datos objetivos. El Sistema de Seguridad Nacional enfocará sus esfuerzos en la alerta temprana, la formulación de medidas preventivas y la coordinación reforzada entre todos los entes públicos. Esto incluye un marco de cogobernanza con las Comunidades Autónomas en cuestiones donde las competencias son autonómicas o compartidas.

Para la gestión de crisis de carácter transnacional será necesario potenciar los procedimientos de actuación coordinada de la Unión Europea, a través de mecanismos de monitorización de riesgos y el desarrollo de bases de datos conjuntas para la identificación y valoración de potenciales riesgos y amenazas.

El segundo objetivo es favorecer la dimensión de seguridad de las capacidades tecnológicas y de los sectores estratégicos. Esto requiere incorporar aspectos de seguridad en el desarrollo tecnológico desde su concepción. Asimismo, implica constantes adaptaciones y actualizaciones que afectan al ámbito regulatorio, a los controles de calidad y a la formación.

El fomento de iniciativas y proyectos de I+D+i es fundamental para que, tanto desde los organismos públicos como desde el sector empresarial, se promueva el desarrollo tecnológico orientado a prevenir y a combatir los riesgos y las amenazas en sectores estratégicos, como la seguridad alimentaria, la salud o la ciberseguridad. En particular, es necesario tomar conciencia del potencial estratégico de la Inteligencia Artificial y la importancia de esta tecnología como puntal de la Seguridad Nacional.

El tercer objetivo es desarrollar la capacidad de prevención, disuasión, detección y respuesta de España frente a estrategias híbridas, en un contexto de seguridad en el que las amenazas convencionales se alternan con el uso combinado de vectores económicos, tecnológicos, diplomáticos y de información, entre otros, como elementos de presión y desestabilización.

La Estrategia establece tres ejes estratégicos sobre los que se articulan las líneas de acción (L.A.) de la política de Seguridad Nacional:

– Una España que protege la vida de las personas y sus derechos y libertades, así como el orden constitucional.
– Una España que promueve la prosperidad y el bienestar de los ciudadanos.
– Una España que participa en la preservación de la paz y la seguridad internacional y defiende sus intereses estratégicos.

Gran parte de las líneas de acción incorporan elementos de alineación o convergencia con medidas europeas e internacionales, reflejo de la naturaleza global de la mayoría de las amenazas a la Seguridad Nacional.

La cultura de Seguridad Nacional es un complemento importante para el desarrollo y la consolidación de la Política de Seguridad Nacional, ya que la concienciación social contribuye a fortalecer la resiliencia de la sociedad y del Estado. Para ello, es necesario implementar las acciones incluidas en el Plan Integral de Cultura de Seguridad Nacional, a través de la colaboración de las administraciones públicas, el sector privado y la sociedad civil, en cuatro ámbitos de actuación: formación; comunicación pública y divulgación; relevancia exterior; y participación activa de la ciudadanía y de las organizaciones de la sociedad civil.

*Primer eje: Una España que protege la vida de las personas y sus derechos y libertades, así como el orden constitucional*

El fortalecimiento de las capacidades de los componentes fundamentales de la Seguridad Nacional –la Defensa Nacional, la Acción Exterior y la Seguridad Pública, con el apoyo de los Servicios de Inteligencia e Información del Estado– junto al refuerzo de la Sanidad Pública, la Protección Civil y la protección de las Infraestructuras Críticas son claves para hacer frente a las amenazas que afectan a los valores e intereses de España y contribuyen a su cohesión territorial.

Disuasión y defensa

La protección de la soberanía nacional, la población y su libertad requiere disponer de unas adecuadas capacidades militares, tecnológicamente avanzadas, que contribuyan a garantizar una disuasión creíble, desde la premisa de que la diplomacia y el Derecho Internacional son los principales instrumentos para proteger los intereses nacionales.

Esta mejora de las capacidades militares asociadas a la disuasión y la defensa ha de ser sostenible en el largo plazo, lo que exige disponer de un marco presupuestario estable. Asimismo, demanda una política activa de colaboración público-privada que apoye firmemente al sector industrial y tecnológico de la seguridad y la defensa en España.

La adaptación al nuevo escenario estratégico requiere garantizar capacidades que cubran todo el espectro de la crisis o el conflicto, desde las operaciones de combate hasta el apoyo a autoridades civiles en la gestión de crisis.

España contribuirá a la capacidad de la OTAN para desarrollar tareas de defensa colectiva, de gestión de crisis y de respuesta a desastres y catástrofes, dentro de una visión global que incorpora todos los aspectos del conflicto y las operaciones. Además, trabajará para integrar los sistemas de mando y control nacionales con los internacionales, aliados, correspondientes.

Para la disuasión y la defensa:

L.A. 1. Asegurar las capacidades militares necesarias para proporcionar una disuasión creíble y una respuesta eficaz en todo el espectro de la crisis o conflicto, garantizando su sostenibilidad en el tiempo bajo un marco presupuestario, suficiente y estable.

L.A. 2. Reforzar las capacidades de defensa a través de la investigación, el desarrollo y la innovación tecnológica como vectores de ventaja estratégica.

L.A. 3. Desarrollar el sector industrial de la defensa, la seguridad y el espacio, así como las tecnologías duales, mediante la cooperación público-privada y el aprovechamiento de sinergias con las herramientas existentes tanto en el marco nacional como de las Organizaciones Internacionales de Seguridad y Defensa a las que pertenece España, en particular los Fondos Europeos de Defensa y la Cooperación Estructurada Permanente de la Unión Europea.

Lucha contra el terrorismo y la radicalización violenta

Para reducir la vulnerabilidad de la sociedad es necesario neutralizar la amenaza que representan las acciones terroristas dirigidas contra los ciudadanos y los intereses de España dentro y fuera de sus fronteras y hacer frente a los procesos de radicalización que conducen al extremismo violento.

Además del papel de las Fuerzas y Cuerpos de Seguridad y de los Servicios de Inteligencia, la participación de las Fuerzas Armadas en misiones internacionales contra el terrorismo resulta fundamental para hacer frente a esta amenaza, así como una actuación coordinada de todos estos actores.

Los principales vectores de la amenaza y en los que se deben concentrar los esfuerzos son los actores solitarios, los combatientes terroristas extranjeros, la propaganda yihadista y extremista y la radicalización en las prisiones. También es necesario participar en iniciativas internacionales cuyo objetivo es impedir que determinadas zonas puedan convertirse en refugio para terroristas, bien sea por la debilidad de los gobiernos de esos territorios o por la afinidad ideológica de estos con los grupos yihadistas.

La actuación en materia de lucha contra el terrorismo se estructura en cuatro pilares: prevenir, proteger, perseguir y preparar la respuesta, que sirven como base para el desarrollo de las principales medidas contra esta amenaza. Así lo establece la Estrategia Nacional contra el Terrorismo 2019, que es la principal referencia nacional en esta materia y consta de dos desarrollos fundamentales: el Plan Estratégico Nacional de Prevención y Lucha Contra la Radicalización Violenta 2020 y el Plan Estratégico Nacional de Lucha Contra la Financiación del Terrorismo 2020.

En relación con la radicalización, es fundamental reforzar la colaboración ciudadana, siendo prioritaria la constitución de las Oficinas de Prevención en las Delegaciones de Gobierno y de los grupos territoriales de prevención en las Juntas Locales de Seguridad. En el caso de aquellas Comunidades Autónomas que ya dispongan de programas específicos, la coordinación se llevará a cabo de acuerdo a su estructura y diseño.

Por otro lado, se requiere fomentar y actualizar las herramientas para la prevención, la detección y el seguimiento de los procesos de radicalización, en general, con la colaboración ciudadana y en los centros penitenciarios, en particular, con programas de tratamiento y evaluación del riesgo de radicalización.

Respecto a la financiación del terrorismo, el desarrollo de la interoperabilidad entre los sistemas existentes en las distintas instituciones permitirá identificar a los actores implicados y posibilitar la trazabilidad completa de los fondos que sean susceptibles de emplearse con fines terroristas.

Para atajar las actividades terroristas o de radicalización en la red y cumplir con la normativa europea, se creará la Unidad Nacional de Notificación de Contenidos de Internet para la monitorización y retirada de contenidos ilícitos de Internet.

Adicionalmente, se debe actualizar el plan de protección y prevención antiterrorista exterior centrado en la asistencia a los ciudadanos o activos españoles víctimas de ataques terroristas fuera de España.

Para la lucha contra el terrorismo y la radicalización violenta:

L.A. 4. Desarrollar herramientas y capacidades que refuercen la ejecución de investigaciones en el ámbito de la lucha contra el terrorismo por parte de los organismos implicados, así como reforzar la coordinación de esos organismos.

L.A. 5. Potenciar el desarrollo e implementación del Plan Estratégico Nacional de Prevención y Lucha Contra la Radicalización Violenta (PENCRAV) y del Plan Estratégico Nacional de Lucha Contra la Financiación del Terrorismo (PENCFIT).

L.A. 6. Incrementar la contribución española en iniciativas de ámbito internacional relativas al contraterrorismo y promover la capacitación y fortalecimiento de organismos e instituciones con competencias en contraterrorismo en países especialmente afectados.

L.A. 7. Potenciar las capacidades de prevención en la lucha contraterrorista de las actividades vinculadas al terrorismo y a extremismos violentos, especialmente en Internet y redes sociales.

L.A. 8. Actualizar el plan de protección y prevención antiterrorista en sus dimensiones interior y exterior.

### Actuación frente a situaciones de crisis

Ante amenazas que trasciendan los marcos ordinarios de respuesta, la gestión de crisis del Sistema de Seguridad Nacional ha de contar, en primer lugar, con un sistema de información para el apoyo a la decisión basado en el análisis de indicadores que proporcione alerta temprana sobre los riesgos y amenazas a la Seguridad Nacional. En segundo lugar, requiere una red de comunicaciones segura, que permita integrar la información y ofrecer una respuesta desde una estructura de mando y control nacional. En tercer lugar, es necesario disponer de un catálogo actualizado de recursos humanos y materiales y de planes de preparación y disposición de estos para hacer frente a las situaciones de crisis. Todo ello, en un marco normativo actualizado de Seguridad Nacional.

Por otro lado, la dependencia del exterior en el suministro de recursos estratégicos supone una vulnerabilidad que se ha de paliar con una adecuada política industrial, tanto a nivel nacional como europeo, que apoye la capacidad de producción de recursos nacionales.

Entre las medidas de carácter sectorial, la lucha contra las epidemias y pandemias demanda la modernización del sistema de vigilancia epidemiológica nacional, a partir de las lecciones aprendidas en la gestión de la pandemia de la COVID-19. Es necesario actualizar el sistema de vigilancia nacional de Salud Pública para permitir una respuesta ágil y acertada.

En el Sistema Nacional de Protección Civil, la consolidación de estructuras funcionales y redes de coordinación, junto con la asignación de los recursos necesarios, contribuirán a fortalecer la gestión de emergencias y catástrofes, de acuerdo con lo establecido en el Plan Estatal General de Emergencias de Protección Civil. Asimismo, es importante asegurar el intercambio de información permanente y en tiempo real entre el Sistema Nacional de Protección Civil y el Sistema de Seguridad Nacional en caso de catástrofe.

Las Infraestructuras Críticas constituyen el eje sobre el que se articula la resiliencia física de un país. Incluyen los sectores de la salud, energético, de alimentación, de transportes y el suministro de agua entre otros. Su funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Es preciso impulsar la dimensión preventiva del Sistema Nacional de Protección de las Infraestructuras Críticas, con especial énfasis en la protección de los sistemas informáticos de las Infraestructuras Críticas y operadores de servicios esenciales frente a ciberamenazas. En este sentido, la colaboración público-privada y el I+D+i para robustecer la resiliencia frente a ciberataques es clave.

Las Ciudades Autónomas de Ceuta y Melilla, por su localización geográfica en el continente africano y por la especificidad de su frontera española y europea, requieren de una especial atención por parte de la Administración General del Estado para garantizar la seguridad y el bienestar de sus ciudadanos.

Para hacer frente a situaciones de crisis:

L.A. 9. Desarrollar el modelo de gestión integral de crisis en el Sistema de Seguridad Nacional a través de la elaboración de un reglamento de gestión de crisis; la implantación de un sistema de alerta temprana basado en indicadores; la creación de un catálogo de recursos y de planes de preparación y disposición de recursos; y el diseño de un Plan de ejercicios de preparación en el marco de la Seguridad Nacional.

L.A.10. Crear la Reserva Estratégica basada en capacidades nacionales de producción industrial con una triple orientación:

a) Identificar los recursos industriales esenciales de las diferentes Administraciones Públicas y del sector privado correspondientes a sus respectivos ámbitos competenciales.

b) Garantizar el suministro de aquellos bienes y servicios que sean considerados como de primera necesidad y carácter estratégico.

c) Salvaguardar la base industrial que suministra recursos de primera necesidad y carácter estratégico, como pudieran ser componentes electrónicos, materiales estratégicos, maquinaria de alta tecnología, aeronáutica, semiconductores, química esencial, equipos agrarios avanzados, tecnología de la comunicación o equipos sanitarios, entre otros.

L.A. 11. Modernizar el sistema de vigilancia nacional de Salud Pública a través de la renovación de las tecnologías sanitarias y los sistemas de información. La Estrategia Digital del Servicio Nacional de Salud incluirá medidas para mejorar la prevención, el diagnóstico, la vigilancia y la gestión de la salud en un marco de cogobernanza con las Comunidades Autónomas.

L.A. 12. Elaborar un Plan Integral de Seguridad para Ceuta y Melilla.

### Contrainteligencia, lucha contra las campañas de desinformación y acción frente a las injerencias del exterior

Para proteger los intereses de España se debe prevenir, detectar y neutralizar las agresiones encubiertas procedentes del exterior, cuyo objetivo es obtener información sensible de forma ilegal para atacar la imagen internacional de España o realizar acciones de injerencia.

Esto incluye reforzar e integrar las capacidades de los Servicios de Inteligencia para hacer frente a las operaciones en el ciberespacio y al espionaje, amenazas que cada vez cobran mayor relevancia por su capacidad de desestabilizar las instituciones del Estado y por su impacto sobre la vida y libertad de los ciudadanos. Para ello, resulta necesario que los Servicios de Inteligencia españoles se mantengan al nivel de los más relevantes de la Unión Europea. En este sentido, se potenciarán sus capacidades humanas y tecnológicas, de manera que se sigan aprovechando las ventajas vinculadas a una adecuada gestión y tratamiento del dato, como la Inteligencia Artificial la computación cuántica o la nube. Además, se velará por la adecuada actualización legislativa para garantizar tanto los derechos de los ciudadanos españoles, como la capacidad de los Servicios de actuar en su defensa.

La protección del patrimonio científico y tecnológico requerirá un esfuerzo adicional por parte del Centro Nacional de Inteligencia (CNI), del Centro Criptológico Nacional (CCN) y de la Oficina Nacional de Seguridad (ONS). En este sentido, será esencial un creciente esfuerzo en las actividades de sensibilización frente a las actuaciones de Servicios de Inteligencia hostiles en el ámbito de la industria nacional y de los sectores estratégicos. Asimismo, el refuerzo de la ONS será fundamental, en línea con la creciente importancia de la protección de la información clasificada como recurso esencial para la Seguridad Nacional. Medida que, a su vez, favorecerá la participación de la industria española en programas clasificados en el exterior.

Por otro lado, hacer frente a las campañas de desinformación, que socavan la confianza a de los ciudadanos en las instituciones democráticas y conducen a la polarización social, requiere hacer un uso sistemático de la detección, alerta temprana y notificación así como la coordinación de la respuesta, siempre en línea con las pautas y el trabajo desarrollado en el seno de la Unión Europea. La colaboración público-privada, especialmente con los medios de comunicación y proveedores de redes sociales, y la sensibilización de la ciudadanía son aspectos clave a la hora de detectar y hacer frente a las campañas de desinformación.

Las iniciativas nacionales estarán coordinadas con los planes existentes a nivel europeo, como el Plan de Acción contra la Desinformación y el Plan de Acción para la Democracia Europea.

Para la Contrainteligencia, lucha contra las campañas de desinformación y acción frente a las injerencias del exterior:

L.A. 13. Elaborar una Estrategia Nacional de Lucha contra las campañas de desinformación.

L.A. 14. Incrementar las capacidades de los Servicios de Inteligencia españoles frente a los ataques de los Servicios de Inteligencia hostiles, en especial en el ciberespacio.

L.A. 15. Potenciar las capacidades de la Oficina Nacional de Seguridad y garantizar un marco legal adecuado para la protección de la información clasificada.

L.A. 16. Reforzar la cooperación internacional en materia de contrainteligencia.

*Segundo eje: Una España que promueve la prosperidad y el bienestar de los ciudadanos*

En un contexto marcado por la necesidad de recuperación económica, el crecimiento inclusivo y la creación de empleo requieren políticas de inversión en innovación y competitividad con visión de futuro, de manera que contribuyan a reforzar la resiliencia de la sociedad a largo plazo.

Seguridad de los espacios comunes globales

El normal desarrollo de la actividad social y económica depende, en gran medida, de la libre circulación de personas, bienes, servicios e ideas que se realizan a través de los espacios comunes globales: el ciberespacio, el espacio marítimo y el espacio aéreo y ultraterrestre.

Son espacios de conexión caracterizados por su apertura funcional, la carencia de fronteras físicas y su fácil accesibilidad. Por otro lado, en los espacios comunes globales resulta difícil la atribución de cualquier acción irregular o delictiva, dada su extensión, su débil regulación y la ausencia de soberanía.

Ciberespacio:

En términos de ciberseguridad, se requiere garantizar el uso seguro y fiable del ciberespacio, para proteger los derechos y las libertades de los ciudadanos y promover el progreso socio económico. Para ello es importante incrementar las capacidades (tecnológicas, humanas y económicas) de la ciberseguridad nacional dirigidas a la prevención, detección, respuesta, recuperación, investigación y defensa activa.

La Carta de Derechos Digitales supone un paso adelante en la protección de los derechos de la ciudadanía en el entorno virtual actual. Esto incluye el reconocimiento del derecho a la igualdad en los ámbitos digitales, la no discriminación y la no exclusión.

En la Administración pública, es ineludible avanzar en el modelo de gobernanza de la ciberseguridad nacional, sobre la base de una mayor eficiencia en los recursos y la integración de las capacidades nacionales. En este sentido, el Centro de Operaciones de Ciberseguridad permitirá, mediante la prestación de servicios horizontales, aumentar las capacidades de vigilancia, detección y respuesta ante ciberataques contra la Administración General del Estado y sus organismos públicos, así como contra las administraciones autonómicas y locales. Un aspecto relevante será el desarrollo de las infraestructuras de ciberseguridad en las Comunidades y Ciudades Autónomas.

Prioridades adicionales son la creación de un sistema de observación y medición de la situación de la ciberseguridad nacional y la puesta en marcha de una plataforma nacional de notificación y seguimiento de ciberincidentes que permita medir el intercambio de información entre organismos públicos y privados en tiempo real.

Por otro lado, será preciso implementar los nuevos requerimientos previstos en el marco de la Unión Europea en la Estrategia de Ciberseguridad de la UE para la Era Digital y en la adecuación de las nuevas propuestas normativas, que han de incluir la legislación necesaria para la protección de las redes y sistemas.

Espacio marítimo:

La Estrategia de Seguridad Marítima promueve un enfoque integral que potencie la actuación coordinada y cooperativa de las diferentes Administraciones; la adopción de medidas para fortalecer la capacidad de actuación del Estado en la mar y en su litoral; el impulso de la colaboración con el sector privado; y, por último, el fomento de la cooperación internacional, en particular a través de la aplicación de las iniciativas de la Organización Marítima Internacional, la Estrategia de Seguridad Marítima de la Unión Europea y la Estrategia Marítima de la OTAN.

Una de las prioridades en el ámbito marítimo es la seguridad de la flota mercante y pesquera española en aguas jurisdiccionales e internacionales.

Además, en el marco de la Seguridad Nacional, es indispensable una planificación preventiva que proporcione respuestas efectivas ante situaciones de complejidad que requieran una actuación concertada de los diversos organismos implicados en el dominio marítimo. Esto supone introducir tecnologías de Inteligencia Artificial en sistemas, plataformas y sensores de vigilancia marítima para la modernización de las capacidades marítimas.

Espacio aéreo y ultraterrestre:

Es esencial garantizar la seguridad del espacio aéreo y ultraterrestre en un marco compartido y orientado a prevenir los riesgos y amenazas que en ellos se desarrollan, así como neutralizar sus consecuencias, conforme a los principios de eficiencia y máxima coordinación, tanto en el empleo de las capacidades de análisis y evaluación como en las de respuesta ante los riesgos y las amenazas.

La seguridad frente a la amenaza de vehículos aéreos no tripulados precisa de acciones urgentes, dada su proliferación.

El sector espacial es clave para la Seguridad Nacional por los servicios que proporciona. Es preciso desarrollar una política de seguridad en el espacio ultraterrestre basada en la cooperación internacional, que tenga como eje la colaboración entre todos los actores implicados. En este sentido, España debe incorporarse a todas aquellas iniciativas internacionales orientadas a preservar el uso pacífico del espacio ultraterrestre, con especial atención a los programas espaciales de la Unión Europea.

Ante la evolución acelerada del sector, debe alcanzarse un reparto eficaz y eficiente de competencias espaciales entre los diversos organismos involucrados. La creación de una Agencia Espacial Española contribuirá a ordenar las competencias y establecer una política nacional que sirva de guía, tanto al sector público como al privado. Así, se podrá maximizar el rendimiento de las inversiones, fomentar espacios de colaboración públicos y privados, facilitar el uso dual de las capacidades espaciales y potenciar el sector de la industria espacial nacional de forma clara y coherente. Además, la Agencia representará internacionalmente a España en el sector espacial.

Para la seguridad de los espacios comunes globales:

En el ciberespacio:

L.A.17. Avanzar en la integración del modelo de gobernanza de la ciberseguridad en el marco del Sistema de Seguridad Nacional.

En el espacio marítimo:

L.A. 18. Elaborar escenarios de riesgo y planes de preparación y respuesta para aquellas situaciones que se consideren de especial interés para la Seguridad Nacional en el ámbito de la seguridad marítima.

En el espacio aéreo y ultraterrestre:

L.A. 19. Crear la Agencia Espacial Española, con un componente dedicado a la Seguridad Nacional, para dirigir el esfuerzo en materia espacial, coordinar de forma eficiente los distintos organismos nacionales con responsabilidades en el sector espacial y unificar la colaboración y coordinación internacional.

Estabilidad económica y financiera

Un contexto económico justo, estable y seguro es condición necesaria para el progreso y favorece la creación de empleo, así como la competitividad de las empresas y la industria española.

La estrategia económica para hacer frente a la crisis derivada de la pandemia está recogida en el Plan de Recuperación, Transformación y Resiliencia. Este Plan traza la hoja de ruta para la modernización de la economía española, la recuperación del crecimiento económico y la creación de empleo tras la crisis de la COVID-19, así como para responder a los retos de la próxima década.

Las medidas que se adopten han de ir acompañadas de una política fiscal robusta y progresiva de acuerdo con el principio de estabilidad presupuestaria y sostenibilidad financiera y que promueva medidas contra la evasión de impuestos, el blanqueo de capitales y la corrupción.

Asimismo, para ejecutar una política preventiva y anticipar posibles crisis, es importante monitorizar los riesgos sistémicos y la publicación de alertas sobre aspectos que puedan afectar a la estabilidad financiera.

Por otra parte, la sostenibilidad del crecimiento económico a medio plazo requiere impulsar la modernización y la productividad del ecosistema industrial español. Este aspecto cobra también sentido en relación a determinados activos estratégicos para la Seguridad Nacional que son objeto de inversión directa extranjera. La tecnología, la salud, el sector aeroespacial o las energías renovables, área esta última en la que España ocupa una posición de liderazgo, son sectores industriales estratégicos para la seguridad. Se han de potenciar, desde una economía abierta, en línea con el marco normativo europeo y el mecanismo de coordinación de la Unión Europea, pero también con vistas a asegurar la cadena de valor, contribuir a una mayor autonomía estratégica y, por tanto, a una mayor resiliencia en situaciones de crisis.

Para la estabilidad económica y financiera:

L.A. 20. Potenciar la modernización y la productividad del ecosistema español industrial, mediante el impulso de la competitividad de sectores estratégicos clave para la Seguridad Nacional, en línea con lo establecido en el Plan de Recuperación, Transformación y Resiliencia.

Lucha contra el crimen organizado y la delincuencia grave

Las políticas públicas contra la criminalidad organizada y la delincuencia grave deben orientarse hacia la identificación temprana de la actividad delictiva, su prevención, persecución y represión efectivas. Para ello, se debe promover la actuación coordinada de los Servicios de Inteligencia, Fuerzas y Cuerpos de Seguridad y autoridades fiscal y judicial. A la lucha directa contra la criminalidad desde las instituciones públicas, debe sumarse además la concienciación social sobre el fenómeno delictivo. En este sentido, en marzo de 2020 se aprobó el Plan Estratégico contra la Criminalidad.

Para neutralizar la economía del crimen organizado, se necesitan instrumentos que mejoren la inteligencia y la detección, además de nuevas capacidades de ciberseguridad. Para ello, hay que establecer un plan estratégico que incluya el blanqueo de capitales y la recuperación y localización de activos.

El desarrollo de un plan contra la trata y la explotación de seres humanos, especialmente de mujeres y niñas, contribuirá a hacer frente a las desigualdades sociales que genera la criminalidad y a la situación de vulnerabilidad en la que se encuentran ciertos colectivos respecto a los delitos de odio.

Además, es indispensable establecer planes específicos de actuación contra el crimen organizado en las áreas geográficas especialmente proclives a su implantación, actuación y arraigo, como se ha hecho con el plan para el Estrecho de Gibraltar.

Por otro lado, se requiere impulsar nuevas vías de prevención, investigación y análisis de la vinculación entre el crimen organizado y el terrorismo.

Para la lucha contra el crimen organizado y la delincuencia grave:

L.A. 21. Elaborar un plan estratégico de lucha contra el enriquecimiento ilícito de las organizaciones criminales y los delincuentes.

L.A. 22. Desarrollar un plan estratégico específico nacional contra la trata y la explotación de seres humanos.

Ordenación de flujos migratorios

La ordenación de los flujos migratorios y la lucha contra las redes de migración irregular y trata de seres humanos deben ser elementos de permanente atención por parte de las Administraciones Públicas, con la implicación del tercer sector y la sociedad civil.

La articulación de mecanismos que mejoren la eficiencia y la integración de todos los esfuerzos y las capacidades de las Administraciones Públicas redundará en una mayor eficacia y coherencia en la gestión migratoria.

Desde una perspectiva integral y preventiva, la colaboración con los países de origen y tránsito es un aspecto indispensable e insustituible para reducir los movimientos migratorios irregulares hacia España. Por ello, resulta esencial reforzar y aumentar los convenios de colaboración en el ámbito bilateral y en el marco de la Unión Europea, en especial en el Magreb, Sahel y África occidental. Además, establecer nuevas vías de migración regular y mejorar las existentes es una parte esencial del compromiso con los países africanos.

La vigilancia y el control de las fronteras es un elemento fundamental en este ámbito. Por un lado, es una responsabilidad compartida, incluidos los países de origen y tránsito, a los que se debe asistir para incrementar sus capacidades y medios. Por otro lado, en cuanto las fronteras exteriores de la Unión Europea, la inmigración irregular es una responsabilidad no solo de los países frontera de la Unión, sino que concierne a todos los socios europeos. Además de las rutas marítimas y terrestres, es imperativo atender a las llegadas aéreas, tanto desde África como desde otros continentes, a los movimientos secundarios hacia o desde España y a la prolongación ilegal de estancia que deriva en inmigración irregular.

Igualmente, es importante la identificación temprana de grupos vulnerables, así como de eventuales beneficiarios de protección internacional, y la mejora de los centros adecuados para su atención.

La optimización de las capacidades de salvamento y rescate en la mar, la atención humanitaria, la recepción y reseña y el tratamiento de los inmigrantes durante todo el ciclo migratorio, incluidos los procesos de determinación de estatus de los solicitantes de protección internacional, requieren actualizar la legislación nacional.

La inclusión de los migrantes es un vector fundamental para lograr una sociedad más próspera, cohesionada y resiliente. Para la consecución de este objetivo, es imprescindible mejorar la coordinación entre los tres niveles de la Administración General del Estado y establecer políticas públicas dirigidas a erradicar cualquier forma de discriminación, racismo o xenofobia.

Para la ordenación de flujos migratorios:

L.A. 23. Establecer un sistema integral y colaborativo de información a nivel de la Administración General del Estado, que permita conocer en tiempo oportuno la situación de los flujos de inmigración, los recursos comprometidos en su gestión, así como las necesidades identificadas.

L.A. 24. Fortalecer la relación y los acuerdos con los países de origen y tránsito para lograr una migración ordenada e impedir el tráfico de seres humanos.

Seguridad energética y transición ecológica

La transición energética hacia un modelo más sostenible, que incorpore un mayor porcentaje de energías renovables y contribuya a lograr la neutralidad climática y una mayor autonomía estratégica, introduce nuevas oportunidades y retos en el escenario energético, que se suman a la necesidad de garantizar la seguridad del abastecimiento y transporte de hidrocarburos en los próximos años.

Las energías renovables y las infraestructuras del sistema energético, en particular las redes eléctricas que las transportan, tienen repercusiones geopolíticas propias. Así, las tecnologías asociadas a la transición energética, las instalaciones y los nuevos materiales, como las tierras raras, están ganando protagonismo frente a recursos más tradicionales como el petróleo y el gas.

Los cambios en la matriz energética conllevan la incorporación de nuevas tecnologías y, en consecuencia, la ampliación y/o profundización de la dependencia de las mismas.

El nuevo paradigma energético obliga a una revisión de la Estrategia de Seguridad Energética Nacional 2015, para una adecuada actualización y encaje en este marco, donde además se han de tener en consideración el Pacto Verde Europeo y los Acuerdos de París de 2015.

El Plan Nacional de Adaptación al Cambio Climático 2021-2030 es el instrumento de planificación básico para promover la acción coordinada y coherente entre departamentos ministeriales, Comunidades Autónomas y entes locales.

Para la seguridad energética y transición ecológica:

L.A. 25. Actualizar la Estrategia de Seguridad Energética Nacional para establecer objetivos y líneas de acción de acuerdo con el contexto de transición ecológica, energética y económica.

*Tercer eje: Una España que participa en la preservación de la paz y seguridad internacional y defiende sus intereses estratégicos*

España es firme defensora del respeto y cumplimiento del Derecho Internacional. Al mismo tiempo, reconoce la necesidad de algunas reformas del sistema internacional. En particular, aboga por una revisión del sistema de las Naciones Unidas, eje central de la acción multilateral concertada para la prevención de conflictos, la acción humanitaria y la consecución de la paz, para lograr una organización más ágil y eficaz, adaptada a los desafíos mundiales actuales.

Asimismo, los mecanismos de gobernanza global son oportunos para gestionar bienes públicos como la salud pública, la seguridad y sanidad alimentaria o el medioambiente.

Un enfoque preventivo y cooperativo de la seguridad es el principal criterio del compromiso de España con la comunidad internacional. Además, España promueve un enfoque integral en la resolución de conflictos en el exterior, basado en una cooperación multidimensional que fortalezca la gobernanza, la seguridad y el progreso.

España incorpora la igualdad de género como un elemento distintivo de su acción exterior, así como el cumplimiento de la Agenda Mujeres, Paz y Seguridad, con el objetivo de avanzar hacia la igualdad real y efectiva en el plano internacional.

Multilateralismo reforzado

España es un país comprometido con la paz y seguridad internacional. Ningún país por sí solo puede hacer frente a amenazas globales del siglo XXI como la lucha contra las pandemias o contra los efectos del cambio climático. Una acción concertada sobre la base de un multilateralismo más fuerte resulta necesaria con la Organización de Naciones Unidas como principal referencia a nivel mundial. Las iniciativas orientadas a que la Organización Mundial de la Salud sea un instrumento más eficaz forman parte de la propuesta española. Además, se ha de impulsar un control de armamentos que responda al mundo multipolar e incorpore a China.

Para el multilateralismo reforzado:

L.A. 26. Potenciar la diplomacia preventiva y el papel de España como actor activo y comprometido en la mediación de conflictos en el exterior.

L.A. 27. Contribuir a la intensificación del apoyo al régimen internacional de no proliferación de armas de destrucción masiva y desarme, a través de la actualización de el régimen internacional de control, exportación y verificación.

L.A. 28. Impulsar la implementación de los objetivos del II Plan Nacional de Acción de Mujeres, Paz y Seguridad de integrar la perspectiva de género y hacer realidad la participación significativa de las mujeres en la prevención, gestión y resolución de conflictos y la consolidación de la paz.

Autonomía estratégica europea

La autonomía estratégica implica un mayor peso geopolítico de la Unión Europea en la esfera mundial, que puede ser utilizado para equilibrar asimetrías de influencia entre grandes actores, promover una gobernanza justa frente a retos globales como el desarrollo tecnológico, el cambio climático o la lucha contra las pandemias y defender sus valores e intereses.

La autonomía estratégica trasciende el ámbito de la defensa. La construcción del marco europeo de la seguridad sanitaria, las acciones para aumentar la resiliencia de las cadenas de suministro, el avance en la seguridad energética o el impulso hacia una soberanía tecnológica forman parte, entre otros, del amplio espectro de políticas tendentes al fortalecimiento de la seguridad europea y del papel de la Unión como actor global. En este sentido, es clave la reducción de las dependencias estratégicas de materias primas y componentes esenciales de las cadenas de valor industriales, a través de la diversificación de la producción y el suministro, el mantenimiento de reservas y el impulso a la producción e inversión en Europa.

Un pilar esencial de la seguridad europea es ahondar en la complementariedad entre la Unión Europea y la OTAN. Una Europa con mayores capacidades contribuye a una Alianza Atlántica más fuerte y viceversa. La asunción por parte de los aliados europeos de una mayor cuota de responsabilidad en materia de seguridad y defensa refuerza el compromiso asumido.

Otro aspecto relevante es el desarrollo de una mayor cooperación policial, militar, de inteligencia y judicial en la Unión Europea para luchar contra el terrorismo, el crimen organizado y la delincuencia grave.

Para la autonomía estratégica europea:

L.A. 29. Promover un liderazgo decidido en la formulación y el desarrollo de la Política Común de Seguridad y Defensa, en línea con las conclusiones que se obtengan del proceso de revisión de la seguridad europea.

L.A. 30. Contribuir a reforzar las capacidades estratégicas autónomas de la Unión Europea, incluida la construcción de la Europa de la Defensa y el desarrollo de capacidades industriales y tecnológicas europeas.

Mayor protagonismo en la OTAN

La defensa colectiva es un elemento central para la Seguridad Nacional. El compromiso de España con el multilateralismo como mejor vía para proteger intereses y valores frente a las amenazas compartidas a la seguridad encuentra su mejor garantía en la participación

española en la OTAN. Una visión integral de los riesgos y amenazas a la seguridad, que incorpore los desafíos que presenta el flanco sur, ha de tener su debido reflejo en la reflexión estratégica que está acometiendo la Organización.

Para un mayor protagonismo en la OTAN:

L.A. 31. Participar activamente en la revisión estratégica acometida por la OTAN de acuerdo a las siguientes acciones:

a) Promover una mayor convergencia con la Unión Europea en políticas tecnológicas.
b) Enfatizar la importancia del flanco Sur, particularmente del Sahel, para la seguridad europea y transatlántica.
c) Mantener la contribución española a las operaciones OTAN en Europa oriental y al sistema de defensa antimisiles como vector de disuasión.

Preservación del medio ambiente, desarrollo sostenible y lucha contra el cambio climático

Los efectos del cambio climático son una de las amenazas más acuciantes para la Seguridad Nacional por su impacto transversal en ámbitos tan heterogéneos como la seguridad energética, las emergencias y catástrofes o los conflictos y desplazamientos de personas a consecuencia de la degradación medioambiental y los desastres naturales.

En particular, un importante nexo con la seguridad se encuentra en los posibles conflictos derivados de los efectos del cambio climático en los países más vulnerables. Por ello, en el Plan Nacional de Adaptación al Cambio Climático se aboga por políticas preventivas de ayuda al desarrollo, que pongan el foco en la construcción de la resiliencia a través de la detección temprana. A tal fin resulta necesaria la identificación de los lugares más vulnerables al cambio climático para priorizar la acción.

Los compromisos adquiridos en los Acuerdos de París de 2015 y la Agenda 2030 encuentran en el Plan Nacional de Acción para la implementación de la Agenda 2030 la principal referencia para avanzar en la lucha contra la crisis climática.

Para la preservación del medio ambiente, el desarrollo sostenible y la lucha contra el cambio climático:

L.A. 32. Integrar la Agenda 2030 en las políticas de cooperación al desarrollo, para contribuir a reforzar las capacidades de los países más vulnerables a prepararse frente al cambio climático.

L.A. 33. Desarrollar los objetivos del área «paz, seguridad y cohesión social» del Plan Nacional de Adaptación al Cambio Climático 2021-2030 relacionados con la prevención de posibles conflictos mediante su detección temprana, con el fin de reconocer aquellas situaciones que puedan suponer amenazas para la paz y la seguridad internacional.

## CAPÍTULO 5

## El Sistema de Seguridad Nacional y la Gestión de Crisis

El quinto capítulo de la Estrategia presenta un modelo integrado para hacer frente a las situaciones de crisis de forma preventiva, ágil y eficaz en el marco del Sistema de Seguridad Nacional.

El Sistema de Seguridad Nacional es el conjunto de órganos, organismos, recursos y procedimientos que posibilitan la acción del Estado en el ejercicio de las funciones para proteger la libertad y el bienestar de sus ciudadanos, garantizar la defensa de España y sus principios y valores constitucionales, y contribuir junto a socios y aliados a la seguridad internacional.

El Consejo de Seguridad Nacional es la pieza angular del Sistema y es el órgano responsable de la dirección y la coordinación de las actuaciones para la gestión de situaciones de crisis. Estas actuaciones están dirigidas a:

– Detectar y valorar los riesgos y amenazas concretos para la Seguridad Nacional.
– Facilitar el proceso de toma de decisiones.
– Asegurar una respuesta óptima y coordinada de los recursos del Estado que sean necesarios.

Para llevarlas a cabo, el Consejo de Seguridad Nacional está asistido por un Comité Especializado de carácter único para el conjunto del Sistema: el Comité de Situación.

El Comité de Situación estará apoyado por el resto de comités especializados, en sus respectivos ámbitos sectoriales, en todo lo relacionado con la valoración de riesgos y amenazas, en el análisis de los posibles escenarios de crisis, en especial de aquellos susceptibles de derivar en una situación de interés para la Seguridad Nacional, y en la evaluación de los resultados.

*Un modelo avanzado de Gestión de Crisis*

En un entorno de seguridad caracterizado por su elevada complejidad y un ritmo acelerado de cambio, se incrementa la probabilidad de que se produzcan eventos de difícil previsión y de gran impacto para la seguridad. Su prevención y gestión demandan instrumentos de detección y alerta temprana capaces de integrar y analizar toda la información disponible.

Enfoque integral que garantice la resiliencia

Un enfoque integral basado en la resiliencia cubre todas las fases de la gestión de crisis, desde un estado de normalidad hasta la recuperación tras una situación de crisis. Esta aproximación implica implementar estructuras y procesos ágiles que permitan la adopción de políticas anticipatorias, con la ayuda de la digitalización del sistema.

Además, el concepto de resiliencia supone una integración multinivel en el modelo de gestión de crisis, que incorpora tanto la coordinación entre todas las Administraciones públicas (estatal, autonómica y local), como entre los ministerios, el sector privado y científico y la sociedad civil.

A estos fines, y alineado con desarrollos similares en la Unión Europea y la OTAN, el Comité de Situación garantizará, en el marco de la gestión de crisis, el enfoque integral gubernamental y social para aumentar la capacidad de resiliencia frente a todo el espectro de los riesgos y las amenazas a la Seguridad Nacional, con especial atención a las estrategias híbridas, dado el carácter multidimensional y coordinado de este tipo de amenazas, que persiguen atentar contra la estabilidad de los Estados y las instituciones.

Estructuras y procesos

En el marco del Sistema de Seguridad Nacional, la dirección y coordinación de la gestión de crisis es función del Consejo de Seguridad Nacional, asistido por el Comité de Situación.

El Departamento de Seguridad Nacional apoya al Comité de Situación mediante la integración y el análisis de información procedente de todas las autoridades y organismos, la alerta temprana, el seguimiento de la situación y el asesoramiento técnico preventivo y las acciones de respuesta. Este apoyo se materializará a través de los mecanismos de enlace y coordinación del Sistema de Seguridad Nacional, tanto de carácter permanente como de coordinación reforzada. Así, se podrá activar una célula de coordinación, formada por representantes de todos los ministerios y organismos implicados en la respuesta y conducción de la crisis.

Además, el Departamento de Seguridad Nacional se constituye como punto de entrada y relación con los sistemas de gestión de crisis a nivel político-estratégico de la Unión Europea (Dispositivo de Respuesta Política Integrada a las Crisis) y de la OTAN, salvo en lo relativo a las implicaciones de la Defensa Nacional o en materia de Protección Civil.

A los efectos de una adecuada preparación y adiestramiento, conviene realizar ejercicios de gestión de crisis en el plano político-estratégico con carácter periódico. Estos ejercicios tendrán como objetivo general activar la estructura y los procedimientos del Sistema de Seguridad Nacional, ejercitando la gestión de crisis ante una situación de interés para la Seguridad Nacional.

Asimismo, los miembros del Sistema de Seguridad Nacional participarán en los ejercicios de las organizaciones internacionales cuando así sea preciso.

Desarrollo del Sistema

Para el desarrollo de capacidades nacionales para hacer frente a situaciones de crisis, se acometerán las siguientes iniciativas:

– Catálogo de recursos de la Seguridad Nacional. Se elaborará un catálogo dinámico de recursos de los sectores estratégicos del Estado que puedan ser puestos a disposición de las autoridades competentes. En su elaboración participará tanto el sector público como el privado.

A dichos efectos, las Comunidades Autónomas elaborarán sus catálogos específicos de recursos, que se integrarán en el estatal, sobre la base de sus propias competencias y la información facilitada por el Gobierno.

– Planes de preparación y disposición de recursos. Se elaborarán para aquellos escenarios aprobados por el Consejo de Seguridad Nacional que, en base al análisis de los riesgos y las amenazas, así lo aconsejen.

– Sistema de Alerta Temprana basado en indicadores. El modelo integrado para hacer frente a las situaciones de crisis, de forma preventiva, ágil y eficaz, está basado en un sistema que permita la toma de decisiones sobre la base de la información proporcionada por unos datos objetivos de determinación de impactos y la evidencia científica. A tales efectos, se desarrollará un sistema de indicadores críticos de los distintos ámbitos de la Seguridad Nacional, cuya monitorización y análisis permitan desplegar acciones preventivas y, llegado el caso, la ejecución de medidas de respuesta y conducción en tiempo oportuno.

– Integración de la información de Seguridad Nacional. Se adoptarán soluciones tecnológicas basadas en la gestión del conocimiento, y también, con técnicas de Inteligencia Artificial, para la evaluación de la situación de seguridad y el apoyo al análisis estratégico. Estos desarrollos permitirán la integración y el análisis de toda la información relevante, su distribución y puesta a disposición de todos los actores intervinientes en la gestión de la crisis, así como la interoperabilidad de los sistemas involucrados.

– Desarrollo de las comunicaciones especiales de la Presidencia del Gobierno. A través de las comunicaciones especiales, se establecerá un instrumento de gestión para el Sistema de Seguridad Nacional, que se configura como elemento de coordinación y para el intercambio de información clasificada en materia de gestión de crisis.

– Integración de las Comunidades y Ciudades Autónomas en el Sistema de Seguridad Nacional. Corresponde a la Conferencia Sectorial para asuntos de la Seguridad Nacional asumir las funciones como órgano de cooperación entre el Estado y las Comunidades Autónomas en aquellas cuestiones de interés común relacionadas con la Seguridad Nacional.

El acceso a las comunicaciones especiales de la Presidencia del Gobierno de todos los actores intervinientes en una situación de crisis es un requisito imprescindible para su integración efectiva en el Sistema de Seguridad Nacional. De esta forma, en los próximos cinco años se desarrollará un plan de extensión progresiva de esta red.

# § 33

## Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas

Jefatura del Estado
«BOE» núm. 102, de 29 de abril de 2011
Última modificación: 29 de julio de 2022
Referencia: BOE-A-2011-7630

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren,

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

### PREÁMBULO

Los Estados modernos se enfrentan actualmente a diferentes desafíos que confieren a la seguridad nacional un carácter cada vez más complejo. Estos nuevos riesgos, generados, en gran medida, por la globalización, y entre los que se cuentan el terrorismo internacional, la proliferación de armas de destrucción masiva o el crimen organizado, se suman a los ya existentes, de los cuales el terrorismo tradicional venía siendo un exponente.

En este marco, es cada vez mayor la dependencia que las sociedades tienen del complejo sistema de infraestructuras que dan soporte y posibilitan el normal desenvolvimiento de los sectores productivos, de gestión y de la vida ciudadana en general. Estas infraestructuras suelen ser sumamente interdependientes entre sí, razón por la cual los problemas de seguridad que pueden desencadenarse en cascada a través del propio sistema tienen la posibilidad de ocasionar fallos inesperados y cada vez más graves en los servicios básicos para la población.

Hasta tal punto es así, que cualquier interrupción no deseada –incluso de corta duración y debida bien a causas naturales o técnicas, bien a ataques deliberados– podría tener graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además de provocar perturbaciones y disfunciones graves en materia de seguridad, lo que es objeto de especial atención para el Sistema Nacional de Gestión de Situaciones de Crisis.

Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, que están expuestas a una serie de amenazas. Para su protección se hace imprescindible, por un lado, catalogar el conjunto de aquéllas que prestan servicios esenciales a nuestra sociedad y, por otro, diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales

infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

En esa línea, se han emprendido diversas actuaciones a nivel nacional, como la aprobación, por la Secretaría de Estado de Seguridad del Ministerio del Interior, de un primer Plan Nacional de Protección de las Infraestructuras Críticas, de 7 de mayo de 2007, así como la elaboración de un primer Catálogo Nacional de Infraestructuras Estratégicas. Así mismo, con fecha 2 de noviembre de 2007, el Consejo de Ministros aprobó un Acuerdo sobre Protección de Infraestructuras Críticas, mediante el cual se dio un impulso decisivo en dicha materia. El desarrollo y aplicación de este Acuerdo supone un avance cualitativo de primer orden para garantizar la seguridad de los ciudadanos y el correcto funcionamiento de los servicios esenciales.

Paralelamente, existen también una serie de actuaciones desarrolladas a nivel internacional en el ámbito europeo: tras los terribles atentados de Madrid, el Consejo Europeo de junio de 2004 instó a la Comisión Europea a elaborar una estrategia global sobre protección de infraestructuras críticas. El 20 de octubre de 2004 la Comisión adoptó una Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, que contiene propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que les afecten. Con posterioridad, en diciembre de 2004, el Consejo aprobó el PEPIC (Programa europeo de protección de infraestructuras críticas) y puso en marcha una red de información sobre alertas en infraestructuras críticas (Critical Infrastructures Warning Information Network-CIWIN).

En la actualidad, la entrada en vigor de la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE), constituye un importante paso en la cooperación en esta materia en el seno de la Unión. En dicha Directiva se establece que la responsabilidad principal y última de proteger las infraestructuras críticas europeas corresponde a los Estados miembros y a los operadores de las mismas, y se determina el desarrollo de una serie de obligaciones y de actuaciones por dichos Estados, que deben incorporarse a las legislaciones nacionales.

Las actuaciones necesarias para optimizar la seguridad de las infraestructuras se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.

Sin embargo, la seguridad de las infraestructuras críticas exige contemplar actuaciones que vayan más allá de la mera protección material contra posibles agresiones o ataques, razón por la cual resulta inevitable implicar a otros órganos de la Administración General del Estado, de las demás Administraciones Públicas, de otros organismos públicos y del sector privado. Estas infraestructuras críticas dependen cada vez más de las tecnologías de la información, tanto para su gestión como para su vinculación con otros sistemas, para lo cual se basan, principalmente, en medios de información y de comunicación de carácter público y abierto. Es preciso contar, por tanto, con la cooperación de todos los actores involucrados en la regulación, planificación y operación de las diferentes infraestructuras que proporcionan los servicios esenciales para la sociedad, sin perjuicio de la coordinación que ejercerá el Ministerio del Interior en colaboración con las Comunidades Autónomas.

En consecuencia, y dada la complejidad de la materia, su incidencia sobre la seguridad de las personas y sobre el funcionamiento de las estructuras básicas nacionales e internacionales, y en cumplimiento de lo estipulado por la Directiva 2008/114/CE, se hace preciso elaborar una norma cuyo objeto es, por un lado, regular la protección de las infraestructuras críticas contra ataques deliberados de todo tipo (tanto de carácter físico como cibernético) y, por otro lado, la definición de un sistema organizativo de protección de dichas infraestructuras que aglutine a las Administraciones Públicas y entidades privadas afectadas. Como pieza básica de este sistema, la Ley crea el Centro Nacional para la Protección de las Infraestructuras Críticas como órgano de asistencia al Secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a éste como órgano responsable del sistema.

La finalidad de esta norma es, por lo tanto, el establecimiento de medidas de protección de las infraestructuras críticas que proporcionen una base adecuada sobre la que se asiente

una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad para aquéllas.

Sobre esta base, se sustentarán el Catálogo Nacional de Infraestructuras Estratégicas (conforme a la comunicación del Consejo de la Unión Europea de 20 de octubre de 2004, que señala que cada sector y cada Estado miembro deberá identificar las infraestructuras que son críticas en sus respectivos territorios) y el Plan Nacional de Protección de Infraestructuras Críticas, como principales herramientas en la gestión de la seguridad de nuestras infraestructuras.

La Ley consta de 18 artículos, estructurados en 3 Títulos. El Título I se destina a las definiciones de los términos acuñados por la Directiva 2008/114/CE, así como a establecer las cuestiones relativas al ámbito de aplicación y objeto. El Título II se dedica a regular los órganos e instrumentos de planificación que se integran en el Sistema de Protección de las Infraestructuras Críticas. El Título III establece, finalmente, las medidas de protección y los procedimientos que deben derivar de la aplicación de dicha norma. Asimismo, la Ley consta de cuatro Disposiciones Adicionales y cinco Disposiciones Finales.

Si bien el contenido material de la Ley es eminentemente organizativo, especialmente en lo concerniente a la composición, competencias y funcionamiento de los órganos que integran el Sistema de Protección de Infraestructuras Críticas, así como en todo lo relativo a los diferentes planes de protección, se ha optado por dotar a esta norma de rango legal, de acuerdo con el criterio del Consejo de Estado, a fin de poder cubrir suficientemente aquellas obligaciones que la Ley impone y que requieren de una cobertura legal específica.

## TÍTULO I

## Disposiciones generales

**Artículo 1.** *Objeto.*

1. Esta Ley tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las Administraciones Públicas en materia de protección de infraestructuras críticas, previa identificación y designación de las mismas, para mejorar la prevención, preparación y respuesta de nuestro Estado frente a atentados terroristas u otras amenazas que afecten a infraestructuras críticas. Para ello se impulsará, además, la colaboración e implicación de los organismos gestores y propietarios de dichas infraestructuras, a fin de optimizar el grado de protección de éstas contra ataques deliberados de todo tipo, con el fin de contribuir a la protección de la población.

2. Asimismo, la presente Ley regula las especiales obligaciones que deben asumir tanto las Administraciones Públicas como los operadores de aquellas infraestructuras que se determinen como infraestructuras críticas, según lo dispuesto en los párrafos e) y f) del artículo 2 de la misma.

**Artículo 2.** *Definiciones.*

A los efectos de la presente Ley, se entenderá por:

a) Servicio esencial: el servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

b) Sector estratégico: cada una de las áreas diferenciadas dentro de la actividad laboral, económica y productiva, que proporciona un servicio esencial o que garantiza el ejercicio de la autoridad del Estado o de la seguridad del país. Su categorización viene determinada en el anexo de esta norma.

c) Subsector estratégico: cada uno de los ámbitos en los que se dividen los distintos sectores estratégicos, conforme a la distribución que contenga, a propuesta de los Ministerios y organismos afectados, el documento técnico que se apruebe por el Centro Nacional de Protección de las Infraestructuras Críticas.

d) Infraestructuras estratégicas: las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales.

e) Infraestructuras críticas: las infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

f) Infraestructuras críticas europeas: aquellas infraestructuras críticas situadas en algún Estado miembro de la Unión Europea, cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros, todo ello con arreglo a la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE).

g) Zona crítica: aquella zona geográfica continua donde estén establecidas varias infraestructuras críticas a cargo de operadores diferentes e interdependientes, que sea declarada como tal por la Autoridad competente. La declaración de una zona crítica tendrá por objeto facilitar la mejor protección y una mayor coordinación entre los diferentes operadores titulares de infraestructuras críticas o infraestructuras críticas europeas radicadas en un sector geográfico reducido, así como con las Fuerzas y Cuerpos de Seguridad del Estado y las Policías Autonómicas de carácter integral.

h) Criterios horizontales de criticidad: los parámetros en función de los cuales se determina la criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica se evaluarán en función de:

1. El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.

2. El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.

3. El impacto medioambiental, degradación en el lugar y sus alrededores.

4. El impacto público y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

i) Análisis de riesgos: el estudio de las hipótesis de amenazas posibles necesario para determinar y evaluar las vulnerabilidades existentes en los diferentes sectores estratégicos y las posibles repercusiones de la perturbación o destrucción de las infraestructuras que le dan apoyo.

j) Interdependencias: los efectos que una perturbación en el funcionamiento de la instalación o servicio produciría en otras instalaciones o servicios, distinguiéndose las repercusiones en el propio sector y en otros sectores, y las repercusiones de ámbito local, autonómico, nacional o internacional.

k) Protección de infraestructuras críticas: el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del ámbito de su respectiva competencia.

l) Información sensible sobre protección de infraestructuras estratégicas: los datos específicos sobre infraestructuras estratégicas que, de revelarse, podrían utilizarse para planear y llevar a cabo acciones cuyo objetivo sea provocar la perturbación o la destrucción de éstas.

m) Operadores críticos: las entidades u organismos responsables de las inversiones o del funcionamiento diario de una instalación, red, sistema, o equipo físico o de tecnología de la información designada como infraestructura crítica con arreglo a la presente Ley.

n) Nivel de Seguridad: aquel cuya activación por el Ministerio del Interior está previsto en el Plan Nacional de Protección de Infraestructuras Críticas, de acuerdo con la evaluación general de la amenaza y con la específica que en cada supuesto se efectúe sobre cada infraestructura, en virtud del cual corresponderá declarar un grado concreto de intervención de los diferentes organismos responsables en materia de seguridad.

o) Catálogo Nacional de Infraestructuras Estratégicas: la información completa, actualizada, contrastada e informáticamente sistematizada relativa a las características específicas de cada una de las infraestructuras estratégicas existentes en el territorio nacional.

**Artículo 3.** *Ámbito de aplicación.*

1. La presente Ley se aplicará a las infraestructuras críticas ubicadas en el territorio nacional vinculadas a los sectores estratégicos definidos en el anexo de esta Ley.
2. Se exceptúan de su aplicación las infraestructuras dependientes del Ministerio de Defensa y de las Fuerzas y Cuerpos de Seguridad, que se regirán, a efectos de control administrativo, por su propia normativa y procedimientos.
3. La aplicación de esta Ley se efectuará sin perjuicio de:

a) La misión y funciones del Centro Nacional de Inteligencia establecidas en su normativa específica, contando siempre con la necesaria colaboración y complementariedad con aquéllas.
b) Los criterios y disposiciones contenidos en la Ley 25/1964, de 29 de abril, sobre energía nuclear, y normas de desarrollo de la misma, y en la Ley 15/1980, de 22 de abril, de creación del Consejo de Seguridad Nuclear, reformada por la Ley 33/2007, de 7 de noviembre.
c) Lo previsto en el Programa Nacional de Seguridad de la Aviación Civil contemplado en la Ley 21/2003, de 7 de julio, de Seguridad Aérea, y su normativa complementaria.

**Artículo 4.** *El Catálogo Nacional de Infraestructuras Estratégicas.*

1. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, será el responsable del Catálogo Nacional de Infraestructuras Estratégicas (en adelante, el Catálogo), instrumento que contendrá toda la información y valoración de las infraestructuras estratégicas del país, entre las que se hallarán incluidas aquellas clasificadas como Críticas o Críticas Europeas, en las condiciones que se determinen en el Reglamento que desarrolle la presente Ley.
2. La competencia para clasificar una infraestructura como estratégica, y en su caso, como infraestructura crítica o infraestructura crítica europea, así como para incluirla en el Catálogo Nacional de Infraestructuras Estratégicas, corresponderá al Ministerio del Interior, a través de la Secretaria de Estado de Seguridad, incluidas las propuestas, en su caso, del órgano competente de las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público en relación con las infraestructuras ubicadas en su demarcación territorial.

## TÍTULO II

## El Sistema de Protección de Infraestructuras Críticas

**Artículo 5.** *Finalidad.*

1. El Sistema de Protección de Infraestructuras Críticas (en adelante, el Sistema) se compone de una serie de instituciones, órganos y empresas, procedentes tanto del sector público como del privado, con responsabilidades en el correcto funcionamiento de los servicios esenciales o en la seguridad de los ciudadanos.
2. Son agentes del Sistema, con las funciones que se determinen reglamentariamente, los siguientes:

a) La Secretaría de Estado de Seguridad del Ministerio del Interior.
b) El Centro Nacional para la Protección de las Infraestructuras Críticas.
c) Los Ministerios y organismos integrados en el Sistema, que serán los incluidos en el anexo de esta Ley.
d) Las Comunidades Autónomas y las Ciudades con Estatuto de Autonomía.

e) Las Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.

f) Las Corporaciones Locales, a través de la asociación de Entidades Locales de mayor implantación a nivel nacional.

g) La Comisión Nacional para la Protección de las Infraestructuras Críticas.

h) El Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.

i) Los operadores críticos del sector público y privado.

**Artículo 6.** *La Secretaría de Estado de Seguridad.*

La Secretaría de Estado de Seguridad es el órgano superior del Ministerio del Interior responsable del Sistema de Protección de las infraestructuras críticas nacionales.

Para el desempeño de su cometido, el Reglamento de desarrollo de esta Ley determinará sus competencias en la materia, que ejercerá con la asistencia de los demás integrantes del Sistema y, principalmente, del Centro Nacional para la Protección de las Infraestructuras Críticas.

**Artículo 7.** *El Centro Nacional para la Protección de las Infraestructuras Críticas.*

1. Se crea el Centro Nacional para la Protección de las Infraestructuras Críticas (en adelante, el CNPIC) como órgano ministerial encargado del impulso, la coordinación y supervisión de todas las actividades que tiene encomendadas la Secretaría de Estado de Seguridad en relación con la protección de las Infraestructuras Críticas en el territorio nacional.

2. El CNPIC dependerá orgánicamente de la Secretaría de Estado de Seguridad, y sus funciones serán las que reglamentariamente se establezcan.

3. Sin perjuicio de lo dispuesto en el apartado anterior, corresponderá al CNPIC la realización de altas, bajas y modificaciones de infraestructuras en el Catálogo, así como la determinación de la criticidad de las infraestructuras estratégicas incluidas en el mismo.

**Artículo 8.** *Ministerios y organismos integrados en el Sistema de Protección de Infraestructuras Críticas.*

1. Por cada sector estratégico, se designará, al menos, un ministerio, organismo, entidad u órgano de la Administración General del Estado integrado en el Sistema. El nombramiento, alta o baja en éste de un ministerio u organismo con responsabilidad sobre un sector estratégico se efectuará mediante la modificación del anexo de la presente Ley.

2. Los ministerios y organismos del Sistema serán los encargados de impulsar, en el ámbito de sus competencias, las políticas de seguridad del Gobierno sobre los distintos sectores estratégicos nacionales y de velar por su aplicación, actuando igualmente como puntos de contacto especializados en la materia. Para ello, colaborarán con el Ministerio del Interior a través de la Secretaría de Estado de Seguridad.

3. Con tales objetivos, los ministerios y organismos del Sistema desempeñarán las funciones que reglamentariamente se determinen.

4. Un ministerio u organismo del Sistema podrá tener competencias, igualmente, sobre dos o más sectores estratégicos, conforme a lo establecido en el anexo de la presente Ley.

**Artículo 9.** *Delegaciones del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía.*

1. Los Delegados del Gobierno en las Comunidades Autónomas y en las Ciudades con Estatuto de Autonomía tendrán, bajo la autoridad del Secretario de Estado de Seguridad, y en el ejercicio de sus competencias, una serie de facultades respecto de las infraestructuras críticas localizadas en su demarcación.

2. El desarrollo reglamentario de dichas facultades en todo caso incluirá la intervención, a través de las Fuerzas y Cuerpos de Seguridad, en la implantación de los diferentes Planes de Protección Específico y de Apoyo Operativo, así como la propuesta a la Secretaría de Estado de Seguridad de la declaración de una zona como crítica.

3. No obstante lo dispuesto en el apartado primero de este artículo, las Comunidades Autónomas con competencias estatutariamente reconocidas para la protección de bienes y personas y el mantenimiento del orden público desarrollarán, sobre las infraestructuras ubicadas en su territorio, aquellas facultades de las Delegaciones del Gobierno relativas a la coordinación de los cuerpos policiales autonómicos y, en su caso, a la activación por aquellos del Plan de Apoyo Operativo que corresponda para responder ante una alerta de seguridad.

**Artículo 10.** *Comunidades Autónomas y Ciudades con Estatuto de Autonomía.*

1. Las Comunidades Autónomas y Ciudades con Estatuto de Autonomía que ostenten competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público podrán desarrollar, sobre las infraestructuras ubicadas en su demarcación territorial, las facultades que reglamentariamente se determinen respecto a su protección, sin perjuicio de los mecanismos de coordinación que se establezcan.

2. En todo caso, las Comunidades Autónomas mencionadas en el apartado anterior participarán en el proceso de declaración de una zona como crítica, en la aprobación del Plan de Apoyo Operativo que corresponda, y en las reuniones del Grupo de Trabajo Interdepartamental. Asimismo, serán miembros de la Comisión Nacional para la Protección de las Infraestructuras Críticas.

3. Las Comunidades Autónomas no incluidas en los apartados anteriores participarán en el Sistema de Protección de Infraestructuras Críticas y en los Órganos previstos en esta Ley, de acuerdo con las competencias que les reconozcan sus respectivos Estatutos de Autonomía.

**Artículo 11.** *Comisión Nacional para la Protección de las Infraestructuras Críticas.*

1. Se crea la Comisión Nacional para la Protección de las Infraestructuras Críticas (en adelante, la Comisión) como órgano colegiado adscrito a la Secretaría de Estado de Seguridad.

2. La Comisión será la competente para aprobar los diferentes Planes Estratégicos Sectoriales así como para designar a los operadores críticos, a propuesta del Grupo de Trabajo Interdepartamental para la Protección de Infraestructuras Críticas.

3. Sus funciones y composición serán las que reglamentariamente se establezcan.

**Artículo 12.** *Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

1. El Sistema contará con un Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas (en adelante, el Grupo de Trabajo), cuya composición y funciones se determinarán reglamentariamente.

2. Le corresponderá, en todo caso, la elaboración de los diferentes Planes Estratégicos Sectoriales y la propuesta a la Comisión de la designación de los operadores críticos por cada uno de los sectores estratégicos definidos.

**Artículo 13.** *Operadores críticos.*

1. Los operadores considerados críticos en virtud de esta Ley deberán colaborar con las autoridades competentes del Sistema, con el fin de optimizar la protección de las infraestructuras críticas y de las infraestructuras críticas europeas por ellos gestionados. Con ese fin, deberán:

a) Asesorar técnicamente al Ministerio del Interior, a través del CNPIC, en la valoración de las infraestructuras propias que se aporten al Catálogo, actualizando los datos disponibles con una periodicidad anual y, en todo caso, a requerimiento del citado Ministerio.

b) Colaborar, en su caso, con el Grupo de Trabajo en la elaboración de los Planes Estratégicos Sectoriales y en la realización de los análisis de riesgos sobre los sectores estratégicos donde se encuentren incluidos.

c) Elaborar el Plan de Seguridad del Operador en los términos y con los contenidos que se determinen reglamentariamente, debiendo acreditar la implantación de las medidas exigidas por la autoridad competente a través de la certificación oportuna.

d) Elaborar, según se disponga reglamentariamente, un Plan de Protección Específico por cada una de las infraestructuras consideradas como críticas en el Catálogo, debiendo acreditar la implantación de las medidas exigidas por la autoridad competente a través de la certificación oportuna.

e) Designar a un Responsable de Seguridad y Enlace en los términos de la presente Ley.

f) Designar a un Delegado de Seguridad por cada una de sus infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior, comunicando su designación a los órganos correspondientes.

g) Facilitar las inspecciones que las autoridades competentes lleven a cabo para verificar el cumplimiento de la normativa sectorial y adoptar las medidas de seguridad que sean precisas en cada Plan, solventando en el menor tiempo posible las deficiencias encontradas.

h) Constituir un Área de Seguridad del Operador, de la manera que reglamentariamente se determine

2. Será requisito para la designación de los operadores críticos, tanto del sector público como del privado, que al menos una de las infraestructuras que gestionen reúna la consideración de Infraestructura Crítica, mediante la correspondiente propuesta de la que, en todo caso, el CNPIC informará al operador antes de proceder a su clasificación definitiva.

3. La designación como tales de los operadores críticos en cada uno de los sectores o subsectores estratégicos definidos se efectuará en los términos que reglamentariamente se establezcan.

4. Los operadores críticos tendrán en el CNPIC el punto directo de interlocución con el Ministerio del Interior en lo relativo a sus responsabilidades, funciones y obligaciones. En el caso de que los operadores críticos del Sector Público estén vinculados o dependan de una Administración Pública, el órgano competente de ésta podrá erigirse, a través del CNPIC, en el interlocutor con el Ministerio del Interior.

## TÍTULO III

## Instrumentos y comunicación del Sistema

**Artículo 14.** *Instrumentos de planificación del Sistema.*

1. La Protección de las Infraestructuras Críticas frente a las eventuales amenazas que puedan ponerlas en situación de riesgo requiere la adopción y aplicación de los siguientes planes de actuación:

a) El Plan Nacional de Protección de las Infraestructuras Críticas.
b) Los Planes Estratégicos Sectoriales.
c) Los Planes de Seguridad del Operador.
d) Los Planes de Protección Específicos.
e) Los Planes de Apoyo Operativo.

2. El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, elaborará el Plan Nacional de Protección de las Infraestructuras Críticas, siendo éste el documento estructural que permitirá dirigir y coordinar las actuaciones precisas para proteger las infraestructuras críticas en la lucha contra el terrorismo.

3. Los Planes Estratégicos Sectoriales serán asimismo elaborados por el Grupo de Trabajo y aprobados por la Comisión, e incluirán, por sectores, los criterios definidores de las medidas a adoptar para hacer frente a una situación de riesgo.

4. Los Planes de Seguridad del Operador y los Planes de Protección Específicos deberán ser elaborados por los operadores críticos respecto a todas sus infraestructuras clasificadas como Críticas o Críticas Europeas. Se trata de instrumentos de planificación a través de los cuales aquéllos asumen la obligación de colaborar en la identificación de dichas infraestructuras, especificar las políticas a implementar en materia de seguridad de las mismas, así como implantar las medidas generales de protección, tanto las permanentes

como aquellas de carácter temporal que, en su caso, vayan a adoptar para prevenir, proteger y reaccionar ante posibles ataques deliberados contra aquéllas.

5. Los Planes de Apoyo Operativo deberán ser elaborados por el Cuerpo Policial estatal o, en su caso, autonómico, con competencia en la demarcación, para cada una de las infraestructuras clasificadas como Críticas o Críticas Europeas dotadas de un Plan de Protección Específico, debiendo contemplar las medidas de vigilancia, prevención, protección o reacción a prestar, de forma complementaria a aquellas previstas por los operadores críticos.

6. El contenido concreto y el procedimiento de elaboración, aprobación y registro de cada uno de los planes serán los que se determinen reglamentariamente.

**Artículo 15.** *Seguridad de las comunicaciones.*

1. La Secretaría de Estado de Seguridad arbitrará los sistemas de gestión que permitan una continua actualización y revisión de la información disponible en el Catálogo por parte del CNPIC, así como su difusión a los organismos autorizados.

2. Las Administraciones Públicas velarán por la garantía de la confidencialidad de los datos sobre infraestructuras estratégicas a los que tengan acceso y de los planes que para su protección se deriven, según la clasificación de la información almacenada.

3. Los sistemas, las comunicaciones y la información referida a la protección de las infraestructuras críticas contarán con las medidas de seguridad necesarias que garanticen su confidencialidad, integridad y disponibilidad, según el nivel de clasificación que les sea asignado.

**Artículo 16.** *El Responsable de Seguridad y Enlace.*

1. Los operadores críticos nombrarán y comunicarán al Ministerio del Interior un Responsable de Seguridad y Enlace con la Administración en el plazo que reglamentariamente se establezca.

2. En todo caso, el Responsable de Seguridad y Enlace designado deberá contar con la habilitación de Director de Seguridad expedida por el Ministerio del Interior según lo previsto en la normativa de seguridad privada o con la habilitación equivalente, según su normativa específica.

3. Las funciones específicas del Responsable de Seguridad y Enlace serán las previstas reglamentariamente.

**Artículo 17.** *El Delegado de Seguridad de la Infraestructura Crítica.*

1. Los operadores con Infraestructuras consideradas Críticas o Críticas Europeas por el Ministerio del Interior comunicarán a las Delegaciones del Gobierno o, en su caso, al órgano competente de la Comunidad Autónoma con competencias estatutariamente reconocidas para la protección de personas y bienes y para el mantenimiento del orden público donde aquéllas se ubiquen, la existencia de un Delegado de Seguridad para dicha infraestructura.

2. El plazo para efectuar dicha comunicación, así como las funciones específicas del Delegado de Seguridad de la Infraestructura Crítica, serán los que reglamentariamente se establezcan.

**Artículo 18.** *Seguridad de los datos clasificados.*

El operador crítico deberá garantizar la seguridad de los datos clasificados relativos a sus propias infraestructuras, mediante los medios de protección y los sistemas de información adecuados que reglamentariamente se determinen.

**Disposición adicional primera.** *Normativa y régimen económico aplicable a la Comisión Nacional para la Protección de las Infraestructuras Críticas y al Grupo de Trabajo Interdepartamental para la Protección de las Infraestructuras Críticas.*

En lo no previsto en la presente Ley, se estará a lo dispuesto para el funcionamiento de los órganos colegiados en el Capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo

Común. Así mismo, el funcionamiento y los trabajos de la Comisión, así como del Grupo de Trabajo previstos en la presente norma se llevarán a cabo con cargo a las dotaciones presupuestarias y los medios personales y tecnológicos del Ministerio del Interior, sin que supongan incremento alguno del gasto público.

**Disposición adicional segunda.** *Clasificación de los Planes.*

Los Planes a los que se refiere el artículo 14 de la presente Ley tendrán la clasificación que les corresponda en virtud de la normativa vigente en la materia, la cual deberá constar de forma expresa en el instrumento de su aprobación.

**Disposición adicional tercera.** *Fuerzas y Cuerpos de Seguridad.*

Las referencias efectuadas en la presente Ley a las Fuerzas y Cuerpos de Seguridad incluyen, en todo caso, a los Cuerpos policiales dependientes de las Comunidades Autónomas con competencias estatutarias reconocidas para la protección de personas y bienes y para el mantenimiento del orden público.

**Disposición adicional cuarta.** *Ceuta y Melilla.*

De conformidad con lo establecido en los Estatutos de Autonomía de las Ciudades de Ceuta y Melilla, los Consejos de Gobierno de ambas, de acuerdo con la Delegación del Gobierno respectiva, podrán emitir informes y propuestas en relación con la adopción de medidas específicas sobre las infraestructuras situadas en ellas que sean objeto de la presente Ley.

**Disposición final primera.** *Título competencial.*

Esta Ley se dicta al amparo de la competencia atribuida al Estado en virtud del artículo 149.1.29.ª de la Constitución Española en materia de seguridad pública.

**Disposición final segunda.** *Competencias en materia de Protección Civil.*

Lo dispuesto en esta Ley se entiende sin perjuicio de lo que establezca la normativa autonómica en materia de protección civil, de acuerdo con las competencias correspondientes a cada territorio en virtud de lo dispuesto en los correspondientes Estatutos de Autonomía.

**Disposición final tercera.** *Incorporación de Derecho comunitario.*

Mediante esta Ley y sus ulteriores desarrollos reglamentarios se incorpora al Derecho español la Directiva 2008/114/CE del Consejo, de 8 de diciembre, sobre la identificación y clasificación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.

**Disposición final cuarta.** *Habilitación para el desarrollo reglamentario.*

1. Se habilita al Gobierno para que en plazo de seis meses dicte el Reglamento de la presente Ley.
2. Igualmente se habilita al Gobierno a modificar por Real Decreto, a propuesta del titular del Ministerio del Interior y del titular del Departamento competente por razón de la materia, el Anexo de esta Ley.
3. En el ámbito de sus competencias, las Comunidades Autónomas podrán igualmente elaborar las normas reglamentarias necesarias para el desarrollo de la presente Ley.

**Disposición final quinta.** *Entrada en vigor.*

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## ANEXO

### Sectores estratégicos y Ministerios/Organismos del sistema competentes

| Sector | Ministerio/Organismo del sistema |
|---|---|
| Administración. | Ministerio Presidencia. |
| | Ministerio Interior. |
| | Ministerio Defensa. |
| | Centro Nacional de Inteligencia. |
| | Ministerio Política Territorial y Administración Pública. |
| Espacio. | Ministerio Defensa. |
| Industria nuclear. | Ministerio Industria, Turismo y Comercio. |
| | Consejo de Seguridad Nuclear. |
| Industria química. | Ministerio Interior. |
| Instalaciones de investigación. | Ministerio Ciencia e Innovación. |
| | Ministerio Medio Ambiente, y Medio Rural y Marino. |
| Agua. | Ministerio Medio Ambiente, y Medio Rural y Marino. |
| | Ministerio Sanidad, Política Social e Igualdad. |
| Energía. | Ministerio Industria, Turismo y Comercio. |
| Salud. | Ministerio Sanidad, Política Social e Igualdad. |
| | Ministerio Ciencia e Innovación. |
| Tecnologías de la Información y las Comunicaciones (TIC). | Ministerio Industria, Turismo y Comercio. |
| | Ministerio Defensa. |
| | Centro Nacional de Inteligencia. |
| | Ministerio Ciencia e Innovación. |
| | Ministerio Política Territorial y Administración Pública. |
| Transporte. | Ministerio Fomento. |
| Alimentación. | Ministerio Medio Ambiente, y Medio Rural y Marino. |
| | Ministerio Sanidad, Política Social e Igualdad. |
| | Ministerio Industria, Turismo y Comercio. |
| Sistema financiero y tributario. | Ministerio Economía y Hacienda. |

# § 34

## Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información

Jefatura del Estado
«BOE» núm. 218, de 8 de septiembre de 2018
Última modificación: 30 de marzo de 2022
Referencia: BOE-A-2018-12257

I

La evolución de las tecnologías de la información y de la comunicación, especialmente con el desarrollo de Internet, ha hecho que las redes y sistemas de información desempeñen actualmente un papel crucial en nuestra sociedad, siendo su fiabilidad y seguridad aspectos esenciales para el desarrollo normal de las actividades económicas y sociales.

Por ello, los incidentes que, al afectar a las redes y sistemas de información, alteran dichas actividades, representan una grave amenaza, pues tanto si son fortuitos como si provienen de acciones deliberadas pueden generar pérdidas financieras, menoscabar la confianza de la población y, en definitiva, causar graves daños a la economía y a la sociedad, con la posibilidad de afectar a la propia seguridad nacional en la peor de las hipótesis.

El carácter transversal e interconectado de las tecnologías de la información y de la comunicación, que también caracteriza a sus amenazas y riesgos, limita la eficacia de las medidas que se emplean para contrarrestarlos cuando se toman de modo aislado. Este carácter transversal también hace que se corra el riesgo de perder efectividad si los requisitos en materia de seguridad de la información se definen de forma independiente para cada uno de los ámbitos sectoriales afectados.

Por tanto, es oportuno establecer mecanismos que, con una perspectiva integral, permitan mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, facilitando la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea.

II

Con este propósito se dicta este real decreto-ley, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. El real decreto-ley se apoya igualmente en las normas, en los instrumentos de respuesta a incidentes y en los órganos de coordinación estatal existentes en esta materia, lo que, junto a las razones señaladas en el apartado I, justifica que su contenido trascienda el de la propia Directiva.

El real decreto-ley se aplicará a las entidades que presten servicios esenciales para la comunidad y dependan de las redes y sistemas de información para el desarrollo de su actividad. Su ámbito de aplicación se extiende a sectores que no están expresamente incluidos en la Directiva, para darle a este real decreto-ley un enfoque global, aunque se preserva su legislación específica. Adicionalmente, en el caso de las actividades de explotación de las redes y de prestación de servicios de comunicaciones electrónicas y los recursos asociados, así como de los servicios electrónicos de confianza, expresamente excluidos de dicha Directiva, el real decreto-ley se aplicará únicamente en lo que respecta a los operadores críticos.

El real decreto-ley se aplicará, así mismo, a los proveedores de determinados servicios digitales. La Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, los somete a un régimen de armonización máxima, equivalente a un reglamento, pues se considera que su regulación a escala nacional no sería efectiva por tener un carácter intrínsecamente transnacional. La función de las autoridades nacionales se limita, por tanto, a supervisar su aplicación por los proveedores establecidos en su país, y coordinarse con las autoridades correspondientes de otros países de la Unión Europea.

Siguiendo la citada Directiva, el real decreto-ley identifica los sectores en los que es necesario garantizar la protección de las redes y sistemas de información, y establece procedimientos para identificar los servicios esenciales ofrecidos en dichos sectores, así como los principales operadores que prestan dichos servicios, que son, en definitiva, los destinatarios de este real decreto-ley.

Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas adecuadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilicen, aunque su gestión esté externalizada. Las obligaciones de seguridad que asuman deberán ser proporcionadas al nivel de riesgo que afronten y estar basadas en una evaluación previa de los mismos. Las normas de desarrollo de este real decreto-ley podrán concretar las obligaciones de seguridad exigibles a los operadores de servicios esenciales, incluyendo en su caso las inspecciones a realizar o la participación en actividades y ejercicios de gestión de crisis.

El real decreto-ley requiere así mismo que los operadores de servicios esenciales y los proveedores de servicios digitales notifiquen los incidentes que sufran en las redes y servicios de información que emplean para la prestación de los servicios esenciales y digitales, y tengan efectos perturbadores significativos en los mismos, al tiempo que prevé la notificación de los sucesos o incidencias que puedan afectar a los servicios esenciales, pero que aún no hayan tenido un efecto adverso real sobre aquellos, y perfila los procedimientos de notificación.

La notificación de incidentes forma parte de la cultura de gestión de riesgos que la Directiva y el real decreto-ley fomentan. Por ello, el real decreto-ley protege a la entidad notificante y al personal que informe sobre incidentes ocurridos; se reserva la información confidencial de su divulgación al público o a otras autoridades distintas de la notificada y se permite la notificación de incidentes cuando no sea obligada su comunicación.

El real decreto-ley recalca la necesidad de tener en cuenta los estándares europeos e internacionales, así como las recomendaciones que emanen del grupo de cooperación y de la red de CSIRT (Computer Security Incident Response Team) establecidos en el ámbito comunitario por la Directiva, con vistas a aplicar las mejores prácticas aprendidas en estos foros y contribuir al impulso del mercado interior y a la participación de nuestras empresas en él.

Con el fin de aumentar su eficacia y, al tiempo, reducir las cargas administrativas y económicas que estas obligaciones suponen para las entidades afectadas, este real decreto-ley trata de garantizar su coherencia con las que se derivan de la aplicación de otras normativas en materia de seguridad de la información, tanto de carácter horizontal como sectorial, y la coordinación en su aplicación con las autoridades responsables en cada caso.

Respecto a las normas horizontales, destacan los vínculos establecidos con las Leyes 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y 36/2015, de 28 de septiembre, de Seguridad Nacional, y con el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad

en el ámbito de la Administración Electrónica, como normativa especial en materia de seguridad de los sistemas de información del sector público.

Así, se aproxima el ámbito de aplicación de este real decreto-ley al de la Ley 8/2011, de 28 de abril, añadiendo a los sectores previstos por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, los sectores estratégicos adicionales contemplados en esa ley; se apoya en ella para definir el concepto de «servicio esencial», y se atribuye a sus órganos colegiados la determinación de los servicios esenciales y de los operadores de servicios esenciales sujetos al presente real decreto-ley. Teniendo en cuenta la Ley 36/2015, de 28 de septiembre, se atribuye al Consejo de Seguridad Nacional la función de actuar como punto de contacto con otros países de la Unión Europea y un papel coordinador de la política de ciberseguridad a través de la Estrategia de Ciberseguridad Nacional.

III

La Estrategia de Ciberseguridad Nacional con la que España cuenta desde el año 2013, sienta las prioridades, objetivos y medidas adecuadas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información. Dicha Estrategia seguirá desarrollando el marco institucional de la ciberseguridad que este real decreto-ley esboza, compuesto por las autoridades públicas competentes y los CSIRT de referencia, por una parte, y la cooperación público-privada, por otra.

Las autoridades competentes ejercerán las funciones de vigilancia derivadas de este real decreto-ley y aplicarán el régimen sancionador cuando proceda. Así mismo, promoverán el desarrollo de las obligaciones que el real decreto-ley impone, en consulta con el sector y con las autoridades que ejerzan competencias por razón de la materia cuando se refieran a sectores específicos, para evitar la existencia de obligaciones duplicadas, innecesarias o excesivamente onerosas.

Los CSIRT son los equipos de respuesta a incidentes que analizan riesgos y supervisan incidentes a escala nacional, difunden alertas sobre ellos y aportan soluciones para mitigar sus efectos. El término CSIRT es el usado comúnmente en Europa en lugar del término protegido CERT (Computer Emergency Response Team), registrado en EE.UU.

El real decreto-ley delimita el ámbito funcional de actuación de los CSIRT de referencia previstos en ella. Dichos CSIRT son la puerta de entrada de las notificaciones de incidentes, lo que permitirá organizar rápidamente la respuesta a ellos, pero el destinatario de las notificaciones es la autoridad competente respectiva, que tendrá en cuenta esta información para la supervisión de los operadores. En todo caso, el operador es responsable de resolver los incidentes y reponer las redes y sistemas de información afectados a su funcionamiento ordinario.

Se prevé la utilización de una plataforma común para la notificación de incidentes, de tal manera que los operadores no deban efectuar varias notificaciones en función de la autoridad a la que deban dirigirse. Esta plataforma podrá ser empleada también para la notificación de vulneraciones de la seguridad de datos personales según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

IV

Este real decreto-ley consta de siete títulos que contienen, en primer lugar, las definiciones de los términos que se usan a lo largo del texto, la salvaguarda de funciones estatales esenciales, como la seguridad nacional y otras disposiciones generales. A continuación, en el título II se determina la forma y criterios de identificación de los servicios esenciales y de los operadores que los presten a los que se aplicará el real decreto-ley. El orden en que se procederá a su identificación por primera vez se establece en la disposición adicional primera del real decreto-ley. El título III recoge el marco estratégico e institucional de la seguridad de las redes y sistemas de información que se ha descrito anteriormente. Se dedica un precepto específico a la cooperación entre autoridades públicas, como pilar de un ejercicio adecuado de las diferentes competencias concurrentes sobre la materia.

El título IV se ocupa de las obligaciones de seguridad de los operadores, y en él se prevé la aplicación preferente de normas sectoriales que impongan obligaciones equivalentes a las previstas en este real decreto-ley, sin perjuicio de la coordinación ejercida por el Consejo de Seguridad Nacional y del deber de cooperación con las autoridades competentes en virtud de este real decreto-ley.

En el título V, el más extenso, se regula la notificación de incidentes y se presta atención a los incidentes con impacto transfronterizo y a la información y coordinación con otros Estados de la Unión Europea para su gestión. En el título VI, se disponen las potestades de inspección y control de las autoridades competentes y la cooperación con las autoridades nacionales de otros Estados miembros, y en el título VII se tipifican las infracciones y sanciones de este real decreto-ley. En este aspecto, el real decreto-ley se decanta por impulsar la subsanación de la infracción antes que su castigo, el cual, si es necesario dispensarlo, será efectivo, proporcionado y disuasorio, en línea con lo ordenado por la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

El real decreto-ley se cierra con una parte final que incluye las disposiciones adicionales y finales necesarias para completar la regulación.

Esta disposición ha sido sometida al procedimiento de información de normas reglamentarias técnicas y de reglamentos relativos a los servicios de la sociedad de la información, previsto en la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, así como el Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información. Así mismo, se adecúa a los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, conforme a los cuales deben actuar las Administraciones Públicas en el ejercicio de la iniciativa legislativa, como son los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia.

Este real decreto-ley se dicta en virtud de las competencias exclusivas atribuidas al Estado en materia de régimen general de telecomunicaciones y seguridad pública por el artículo 149.1.21.ª y 29.ª de la Constitución.

El real decreto-ley constituye un instrumento constitucionalmente lícito, siempre que el fin que justifica la legislación de urgencia, sea, tal como reiteradamente ha exigido nuestro Tribunal Constitucional (Sentencias 6/1983, de 4 de febrero, F. 5; 11/2002, de 17 de enero, F. 4, 137/2003, de 3 de julio, F. 3 y 189/2005, de 7 julio, F.3), subvenir a un situación concreta, dentro de los objetivos gubernamentales, que por razones difíciles de prever requiere una acción normativa inmediata en un plazo más breve que el requerido por la vía normal o por el procedimiento de urgencia para la tramitación parlamentaria de las Leyes.

Por otro lado, la utilización del instrumento jurídico del real decreto-ley, en el presente caso, además queda justificada por la doctrina del Tribunal Constitucional, que, en su Sentencia 1/2012, de 13 de enero, ha avalado la concurrencia del presupuesto habilitante de la extraordinaria y urgente necesidad del artículo 86.1 de la Constitución, cuando concurra el retraso en la transposición de directivas.

En efecto, el plazo de transposición de la mencionada Directiva (UE) 2016/1148, del Parlamento Europeo y del Consejo, de 6 de julio de 2016, se encuentra ya vencido a 9 de mayo de 2018. La finalización del plazo de transposición de esta Directiva ha motivado la iniciación por parte de la Comisión Europea de un procedimiento formal de infracción n.º 2018/168.

En consecuencia, se entiende que en el conjunto y en cada una de las medidas que se adoptan mediante el real decreto-ley proyectado, concurren, por su naturaleza y finalidad, las circunstancias de extraordinaria y urgente necesidad que exige el artículo 86 de la Constitución como presupuestos habilitantes para la aprobación de un real decreto-ley.

En su virtud, haciendo uso de la autorización contenida en el artículo 86 de la Constitución Española, a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes e Igualdad, del Ministro del Interior y de la Ministra

de Economía y Empresa y previa deliberación del Consejo de Ministros, en su reunión del día 7 de septiembre de 2018,

DISPONGO:

TÍTULO I

**Disposiciones generales**

**Artículo 1.** *Objeto.*

1. El presente real decreto-ley tiene por objeto regular la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y de los servicios digitales, y establecer un sistema de notificación de incidentes.

2. Así mismo, establece un marco institucional para la aplicación de este real decreto-ley y la coordinación entre autoridades competentes y con los órganos de cooperación relevantes en el ámbito comunitario.

**Artículo 2.** *Ámbito de aplicación.*

1. Este real decreto-ley se aplicará a la prestación de:

a) Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

b) Los servicios digitales, considerados conforme se determina en el artículo 3 e), que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.

2. Estarán sometidos a este real decreto-ley:

a) Los operadores de servicios esenciales establecidos en España. Se entenderá que un operador de servicios esenciales está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades.

Así mismo, este real decreto-ley será de aplicación a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

b) Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

3. Este real decreto-ley no se aplicará a:

a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.

b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

**Artículo 3.** *Definiciones.*

A los efectos de este real decreto-ley, se entenderá por:

a) Redes y sistemas de información, cualquiera de los elementos siguientes:

1.º Las redes de comunicaciones electrónicas, tal y como vienen definidas en el número 31 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones;

2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales;

3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

b) Seguridad de las redes y sistemas de información: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

c) Servicio esencial: servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas, que dependa para su provisión de redes y sistemas de información.

d) Operador de servicios esenciales: entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 de este real decreto-ley, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril.

e) Servicio digital: servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

f) Proveedor de servicios digitales: persona jurídica que presta un servicio digital.

g) Riesgo: toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una amenaza que produzca un impacto en términos de operatividad, de integridad física de personas o material o de imagen.

h) Incidente: suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

i) Gestión de incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

j) Representante: persona física o jurídica establecida en la Unión Europea que ha sido designada expresamente para actuar por cuenta de un proveedor de servicios digitales no establecido en la Unión Europea, a la que, en sustitución del proveedor de servicios digitales, pueda dirigirse una autoridad competente nacional o un CSIRT, en relación con las obligaciones que, en virtud de este real decreto-ley, tiene el proveedor de servicios digitales.

k) Norma técnica: una norma en el sentido del artículo 2.1 del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea.

l) Especificación: una especificación técnica en el sentido del artículo 2.4 del Reglamento (UE) n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012.

m) Punto de intercambio de Internet («IXP», por sus siglas en inglés de «Internet eXchange Point»): una instalación de red que permite interconectar más de dos sistemas autónomos independientes, principalmente para facilitar el intercambio de tráfico de Internet. Un IXP permite interconectar sistemas autónomos sin requerir que el tráfico de Internet que pasa entre cualquier par de sistemas autónomos participantes pase por un tercer sistema autónomo, y sin modificar ni interferir de otra forma en dicho tráfico.

n) Sistema de nombres de dominio («DNS», por sus siglas en inglés de «Domain Name System»): sistema distribuido jerárquicamente que responde a consultas proporcionando información asociada a nombres de dominio, en particular, la relativa a los identificadores utilizados para localizar y direccionar equipos en Internet.

o) Proveedor de servicios de DNS: entidad que presta servicios de DNS en Internet.

p) Registro de nombres de dominio de primer nivel: entidad que administra y dirige el registro de nombres de dominio de Internet en un dominio específico de primer nivel.

q) Mercado en línea: servicio digital que permite a los consumidores y a los empresarios, tal y como se definen respectivamente en los artículos 3 y 4 del texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado mediante el Real Decreto Legislativo 1/2007, de 16 de noviembre, celebrar entre sí contratos de compraventa o de prestación de servicios en línea con empresarios, ya sea en un sitio web específico del servicio de mercado en línea, o en un sitio web de un empresario que utilice servicios informáticos proporcionados al efecto por el proveedor del servicio de mercado en línea.

r) Motor de búsqueda en línea: servicio digital que permite a los usuarios hacer búsquedas de, en principio, todos los sitios web o de sitios web en una lengua en concreto, mediante una consulta sobre un tema en forma de palabra clave, frase u otro tipo de entrada, y que, en respuesta, muestra enlaces en los que puede encontrarse información relacionada con el contenido solicitado.

s) Servicio de computación en nube: servicio digital que hace posible el acceso a un conjunto modulable y elástico de recursos de computación que se pueden compartir.

**Artículo 4.** *Directrices y orientaciones comunitarias.*

En la aplicación de este real decreto-ley y en la elaboración de los reglamentos y guías previstos en él se tendrán en cuenta los actos de ejecución de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, así como todas las recomendaciones y directrices emanadas del grupo de cooperación establecido por el artículo 11 de la citada Directiva, y la información sobre buenas prácticas recopiladas por dicho grupo y la red de CSIRT, regulado en el artículo 12 de aquélla.

**Artículo 5.** *Salvaguarda de funciones estatales esenciales.*

Lo dispuesto en este real decreto-ley se entenderá sin perjuicio de las acciones emprendidas para salvaguardar la seguridad nacional y las funciones estatales esenciales, incluyéndose las dirigidas a proteger la información clasificada o cuya revelación fuere contraria a los intereses esenciales del Estado, o las que tengan como propósito el mantenimiento del orden público, la detección, investigación y persecución de los delitos, y el enjuiciamiento de sus autores.

## TÍTULO II

## Servicios esenciales y servicios digitales

**Artículo 6.** *Identificación de servicios esenciales y de operadores de servicios esenciales.*

1. La identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, y su normativa de desarrollo.

La relación de los servicios esenciales y de los operadores de dichos servicios se actualizará, para cada sector, con una frecuencia bienal, en conjunción con la revisión de los planes estratégicos sectoriales previstos en la Ley 8/2011, de 28 de abril.

Se identificará a un operador como operador de servicios esenciales si un incidente sufrido por el operador puede llegar a tener efectos perturbadores significativos en la prestación del servicio, para lo que se tendrán en cuenta, al menos, los siguientes factores:

a) En relación con la importancia del servicio prestado:

1.º La disponibilidad de alternativas para mantener un nivel suficiente de prestación del servicio esencial;

2.º La valoración del impacto de un incidente en la provisión del servicio, evaluando la extensión o zonas geográficas que podrían verse afectadas por el incidente; la dependencia de otros sectores estratégicos respecto del servicio esencial ofrecido por la entidad y la repercusión, en términos de grado y duración, del incidente en las actividades económicas y sociales o en la seguridad pública.

b) En relación con los clientes de la entidad evaluada:

1.º El número de usuarios que confían en los servicios prestados por ella;
2.º Su cuota de mercado.

Reglamentariamente podrán añadirse factores específicos del sector para determinar si un incidente podría tener efectos perturbadores significativos.

2. En el caso de tratarse de un operador crítico designado en cumplimiento de la Ley 8/2011, de 28 de abril, bastará con que se constate su dependencia de las redes y sistemas de información para la provisión del servicio esencial de que se trate.

3. En la identificación de los servicios esenciales y de los operadores de servicios esenciales se tendrán en consideración, en la mayor medida posible, las recomendaciones pertinentes que adopte el grupo de cooperación.

4. Cuando un operador de servicios esenciales ofrezca servicios en otros Estados miembros de la Unión Europea, se informará a los puntos de contacto único de dichos Estados sobre la intención de identificarlo como operador de servicios esenciales.

**Artículo 7.** *Comunicación de actividad por los proveedores de servicios digitales.*

Los proveedores de servicios digitales señalados en el artículo 2 deberán comunicar su actividad a la autoridad competente en el plazo de tres meses desde que la inicien, a los meros efectos de su conocimiento.

## TÍTULO III

## Marco estratégico e institucional

**Artículo 8.** *Marco estratégico de seguridad de las redes y sistemas de información.*

La Estrategia de Ciberseguridad Nacional, al amparo y alineada con la Estrategia de Seguridad Nacional, enmarca los objetivos y las medidas para alcanzar y mantener un elevado nivel de seguridad de las redes y sistemas de información.

La Estrategia de Ciberseguridad Nacional abordará, entre otras cuestiones, las establecidas en el artículo 7 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

A tal efecto, el Consejo de Seguridad Nacional impulsará la revisión de la Estrategia de Ciberseguridad Nacional, de conformidad con lo dispuesto en el artículo 21.1 e) de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

**Artículo 9.** *Autoridades competentes.*

1. Son autoridades competentes en materia de seguridad de las redes y sistemas de información las siguientes:

a) Para los operadores de servicios esenciales:

1.º En el caso de que éstos sean, además, designados como operadores críticos conforme a la Ley 8/2011, de 28 de abril, y su normativa de desarrollo, con independencia del sector estratégico en que se realice tal designación: la Secretaría de Estado de Seguridad, del Ministerio del Interior, a través del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC).

2.º En el caso de que no sean operadores críticos: la autoridad sectorial correspondiente por razón de la materia, según se determine reglamentariamente.

b) Para los proveedores de servicios digitales: la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

c) Para los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público: el Ministerio de Defensa, a través del Centro Criptológico Nacional.

2. El Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, establecerá los mecanismos necesarios para la coordinación de las actuaciones de las autoridades competentes.

**Artículo 10.** *Funciones de las autoridades competentes.*

Las autoridades competentes ejercerán las siguientes funciones:

a) Supervisar el cumplimiento por parte de los operadores de servicios esenciales y de los proveedores de servicios digitales de las obligaciones que se determinen, conforme a lo establecido en el título VI.

b) Establecer canales de comunicación oportunos con los operadores de servicios esenciales y con los proveedores de servicios digitales que, en su caso, serán desarrollados reglamentariamente.

c) Coordinarse con los CSIRT de referencia a través de los protocolos de actuación que, en su caso, se desarrollarán reglamentariamente.

d) Recibir las notificaciones sobre incidentes que sean presentadas en el marco de este real decreto-ley, a través de los CSIRT de referencia, conforme a lo establecido en el título V.

e) Informar al punto de contacto único sobre las notificaciones de incidentes presentadas en el marco de este real decreto-ley, conforme a lo establecido en el artículo 27.

f) Informar, en su caso, al público sobre determinados incidentes, cuando la difusión de dicha información sea necesaria para evitar un incidente o gestionar uno que ya se haya producido, conforme a lo establecido en el artículo 26.

g) Cooperar, en el ámbito de aplicación de este real decreto-ley, con las autoridades competentes en materia de protección de datos de carácter personal, seguridad pública, seguridad ciudadana y seguridad nacional, así como con las autoridades sectoriales correspondientes, conforme a lo establecido en los artículos 14 y 29.

h) Establecer obligaciones específicas para garantizar la seguridad de las redes y sistemas de información y sobre notificación de incidentes, y dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas obligaciones, conforme a lo establecido en los artículos 16 y 19.

i) Ejercer la potestad sancionadora en los casos previstos en el presente real decreto-ley, conforme a lo establecido en el título VII.

j) Promover el uso de normas y especificaciones técnicas, de acuerdo con lo establecido en el artículo 17.

k) Cooperar con las autoridades competentes de otros Estados miembros de la Unión Europea en la identificación de operadores de servicios esenciales entre entidades que ofrezcan dichos servicios en varios Estados miembros.

l) Informar al punto de contacto único sobre incidentes que puedan afectar a otros Estados miembros, en los términos previstos en el artículo 25.

**Artículo 11.** *Equipos de respuesta a incidentes de seguridad informática de referencia.*

1. Son equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia en materia de seguridad de las redes y sistemas de información, los siguientes:

a) En lo concerniente a las relaciones con los operadores de servicios esenciales:

1.º El CCN-CERT, del Centro Criptológico Nacional, al que corresponde la comunidad de referencia constituida por las entidades del ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

2.º El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, al que corresponde la comunidad de referencia constituida por aquellas entidades no incluidas en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

El INCIBE-CERT será operado conjuntamente por el INCIBE y el CNPIC en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos.

3.º El ESPDEF-CERT, del Ministerio de Defensa, que cooperará con el CCN-CERT y el INCIBE-CERT en aquellas situaciones que éstos requieran en apoyo de los operadores de servicios esenciales y, necesariamente, en aquellos operadores que tengan incidencia en la Defensa Nacional y que reglamentariamente se determinen.

b) En lo concerniente a las relaciones con los proveedores de servicios digitales que no estuvieren comprendidos en la comunidad de referencia del CCN-CERT: el INCIBE-CERT.

El INCIBE-CERT será, así mismo, equipo de respuesta a incidentes de referencia para los ciudadanos, entidades de derecho privado y otras entidades no incluidas anteriormente en este apartado 1.

2. Los CSIRT de referencia se coordinarán entre sí y con el resto de CSIRT nacionales e internacionales en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan. En los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

Cuando las actividades que desarrollen puedan afectar de alguna manera a un operador crítico, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de la Oficina de Coordinación Cibernética del Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), de la forma que reglamentariamente se determine.

3. El Centro Criptológico Nacional (CCN) ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (CSIRT) en materia de seguridad de las redes y sistemas de información del sector público comprendido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Los CSIRT de las Administraciones Públicas consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellos en el ejercicio de sus respectivas funciones.

El CCN ejercerá la función de enlace para garantizar la cooperación transfronteriza de los CSIRT de las Administraciones Públicas con los CSIRT internacionales, en la respuesta a los incidentes y gestión de riesgos de seguridad que les correspondan.

**Artículo 12.** *Requisitos y funciones de los CSIRT de referencia.*

1. Los CSIRT deberán reunir las siguientes condiciones:

a) Garantizarán un elevado nivel de disponibilidad de sus servicios de comunicaciones evitando los fallos ocasionales y contarán con varios medios para que se les pueda contactar y puedan contactar a otros en todo momento. Además, los canales de comunicación estarán claramente especificados y serán bien conocidos de los grupos de usuarios y los socios colaboradores.

b) Sus instalaciones y las de los sistemas de información de apoyo estarán situados en lugares seguros.

c) Garantizarán la continuidad de las actividades. Para ello:

1.º Estarán dotados de un sistema adecuado para gestionar y canalizar las solicitudes con el fin de facilitar los traspasos.

2.º Contarán con personal suficiente para garantizar su disponibilidad en todo momento.

3.º Tendrán acceso a infraestructuras de comunicación cuya continuidad esté asegurada. A tal fin, dispondrán de sistemas redundantes y espacios de trabajo de reserva.

d) Deberán tener la capacidad de participar, cuando lo deseen, en redes de cooperación internacional.

2. Los CSIRT desempeñarán como mínimo, las siguientes funciones:

a) Supervisar incidentes a escala nacional.

b) Difundir alertas tempranas, alertas, avisos e información sobre riesgos e incidentes entre los interesados.

c) Responder a incidentes.

d) Efectuar un análisis dinámico de riesgos e incidentes y de conocimiento de la situación.

e) Participar en la red de CSIRT.

3. Los CSIRT establecerán relaciones de cooperación con el sector privado. A fin de facilitar la cooperación, los CSIRT fomentarán la adopción y utilización de prácticas comunes o normalizadas de:

a) Procedimientos de gestión de incidentes y riesgos.
b) Sistemas de clasificación de incidentes, riesgos e información.

**Artículo 13.** *Punto de contacto único.*

El Consejo de Seguridad Nacional ejercerá, a través del Departamento de Seguridad Nacional, una función de enlace para garantizar la cooperación transfronteriza de las autoridades competentes designadas conforme al artículo 9, con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación y la red de CSIRT.

**Artículo 14.** *Cooperación con otras autoridades con competencias en seguridad de la información y con las autoridades sectoriales.*

1. Las autoridades competentes, los CSIRT de referencia y el punto de contacto único consultarán, cuando proceda, con los órganos con competencias en materia de seguridad nacional, seguridad pública, seguridad ciudadana y protección de datos de carácter personal y colaborarán con ellas en el ejercicio de sus respectivas funciones.
2. Consultarán así mismo, cuando proceda, con los órganos con competencias por razón de la materia en cada uno de los sectores incluidos en el ámbito de aplicación de este real decreto-ley, y colaborarán con ellos en el ejercicio de sus funciones.
3. Cuando los incidentes notificados presenten caracteres de delito, las autoridades competentes y los CSIRT de referencia darán cuenta de ello, a través de la Oficina de Coordinación Cibernética del Ministerio del Interior, al Ministerio Fiscal a los efectos oportunos, trasladándole al tiempo cuanta información posean en relación con ello.

**Artículo 15.** *Confidencialidad de la información sensible.*

Sin perjuicio de lo dispuesto en el artículo 5, las autoridades competentes, los CSIRT de referencia y el punto de contacto único preservarán, como corresponda en Derecho, la seguridad y los intereses comerciales de los operadores de servicios esenciales y proveedores de servicios digitales, así como la confidencialidad de la información que recaben de éstos en el ejercicio de las funciones que les encomienda el presente real decreto-ley.
Cuando ello sea necesario, el intercambio de información sensible se limitará a aquella que sea pertinente y proporcionada para la finalidad de dicho intercambio.

## TÍTULO IV

## Obligaciones de seguridad

**Artículo 16.** *Obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar medidas técnicas y de organización, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados en la prestación de los servicios sujetos a este real decreto-ley.
Sin perjuicio de su deber de notificar incidentes conforme al título V, deberán tomar medidas adecuadas para prevenir y reducir al mínimo el impacto de los incidentes que les afecten.
2. El desarrollo reglamentario de este real decreto-ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en el apartado anterior por parte de los operadores de servicios esenciales.
3. Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente, en el plazo que reglamentariamente se establezca, la persona, unidad u órgano

colegiado responsable de la seguridad de la información, como punto de contacto y de coordinación técnica con aquella.

Sus funciones específicas serán las previstas reglamentariamente.

4. Las autoridades competentes podrán establecer mediante Orden ministerial obligaciones específicas para garantizar la seguridad de las redes y sistemas de información empleados por los operadores de servicios esenciales. Así mismo, podrán dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes.

Al elaborar las disposiciones reglamentarias, instrucciones y guías, tendrán en cuenta las obligaciones sectoriales, las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de seguridad de la información, a las que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.

5. Las autoridades competentes deberán coordinarse entre sí y con los diferentes órganos sectoriales con competencias por razón de la materia, en lo relativo al contenido y a la aplicación de las órdenes, instrucciones técnicas y guías orientativas que dicten en sus respectivos ámbitos de competencia, con objeto de evitar duplicidades en las obligaciones exigibles y facilitar su cumplimiento a los operadores de servicios esenciales.

6. Los proveedores de servicios digitales determinarán las medidas de seguridad que aplicarán, teniendo en cuenta, como mínimo, los avances técnicos y los siguientes aspectos:

a) La seguridad de los sistemas e instalaciones;
b) La gestión de incidentes;
c) La gestión de la continuidad de las actividades;
d) La supervisión, auditorías y pruebas;
e) El cumplimiento de las normas internacionales.

Los proveedores de servicios digitales atenderán igualmente a los actos de ejecución por los que la Comisión europea detalle los aspectos citados.

7. Los operadores de servicios esenciales y proveedores de servicios digitales que no siendo operadores críticos se encuentren comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público que utilizan servicios ofrecidos por proveedores de servicios digitales, en particular servicios de computación en nube, podrán exigir a los proveedores de tales servicios medidas de seguridad adicionales, más estrictas que las que dichos proveedores han adoptado en cumplimiento de la legislación en materia de seguridad de las redes y sistemas de información. En particular, las citadas medidas podrán ser exigidas mediante obligaciones contractuales, previo informe preceptivo y vinculante del Centro Criptológico Nacional.

**Artículo 17.** *Normas técnicas.*

Las autoridades competentes promoverán la utilización de regulaciones, normas o especificaciones técnicas en materia de seguridad de las redes y sistemas de información elaboradas en el marco del Reglamento (UE) 1025/2012 del Parlamento Europeo y del Consejo de 25 de octubre de 2012 sobre la normalización europea.

En ausencia de dichas normas o especificaciones, promoverán la aplicación de las normas o recomendaciones internacionales aprobadas por los organismos internacionales de normalización, y, en su caso, de las normas y especificaciones técnicas aceptadas a nivel europeo o internacional que sean pertinentes en esta materia.

**Artículo 18.** *Sectores con normativa específica equivalente.*

Cuando una normativa nacional o comunitaria establezca para un sector obligaciones de seguridad de las redes y sistemas de información o de notificación de incidentes que tengan efectos, al menos, equivalentes a los de las obligaciones previstas en este real decreto-ley, prevalecerán aquellos requisitos y los mecanismos de supervisión correspondientes.

Ello no afectará al deber de cooperación entre autoridades competentes, a la coordinación ejercida por el Consejo de Seguridad Nacional ni, en la medida en que no sea incompatible con la legislación sectorial, a la aplicación del título V sobre notificación de incidentes.

TÍTULO V

**Notificación de incidentes**

**Artículo 19.** *Obligación de notificar.*

1. Los operadores de servicios esenciales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios.

Las notificaciones podrán referirse también, conforme se determine reglamentariamente, a los sucesos o incidencias que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, pero que aún no hayan tenido un efecto adverso real sobre aquéllos.

2. Así mismo, los proveedores de servicios digitales notificarán a la autoridad competente, a través del CSIRT de referencia, los incidentes que tengan efectos perturbadores significativos en dichos servicios.

La obligación de la notificación del incidente únicamente se aplicará cuando el proveedor de servicios digitales tenga acceso a la información necesaria para valorar el impacto de un incidente.

3. Las notificaciones tanto de operadores de servicios esenciales como de proveedores de servicios digitales se referirán a los incidentes que afecten a las redes y sistemas de información empleados en la prestación de los servicios indicados, tanto si se trata de redes y servicios propios como si lo son de proveedores externos, incluso si éstos son proveedores de servicios digitales sometidos a este real decreto-ley.

4. Las autoridades competentes y los CSIRT de referencia utilizarán una plataforma común para facilitar y automatizar los procesos de notificación, comunicación e información sobre incidentes.

5. El desarrollo reglamentario de este real decreto-ley preverá las medidas necesarias para el cumplimiento de lo preceptuado en este artículo por parte de los operadores de servicios esenciales. Las autoridades competentes podrán establecer, mediante Orden ministerial, obligaciones específicas de notificación por los operadores de servicios esenciales. Así mismo, podrán dictar instrucciones técnicas y guías orientativas para detallar el contenido de dichas órdenes.

Al elaborar las disposiciones reglamentarias, instrucciones y guías, se tendrán en cuenta las obligaciones sectoriales, las directrices relevantes que se adopten en el grupo de cooperación y los requisitos en materia de notificación de incidentes a los que estuviera sometido el operador en virtud de otras normas, como la Ley 8/2011, de 28 de abril, y el Esquema Nacional de Seguridad, aprobado por el Real Decreto 3/2010, de 8 de enero.

6. La obligación de notificación de incidentes prevista en los apartados anteriores no obsta al cumplimiento de los deberes legales de denuncia de aquellos hechos que revistan caracteres de delito ante las autoridades competentes, de acuerdo con lo dispuesto en los artículos 259 y siguientes de la Ley de Enjuiciamiento Criminal y teniendo en cuenta lo previsto en el artículo 14.3 de este real decreto-ley.

**Artículo 20.** *Protección del notificante.*

1. Las notificaciones consideradas en este título no sujetarán a la entidad que las efectúe a una mayor responsabilidad.

2. Los empleados y el personal que, por cualquier tipo de relación laboral o mercantil, participen en la prestación de los servicios esenciales o digitales, que informen sobre incidentes no podrán sufrir consecuencias adversas en su puesto de trabajo o con la empresa, salvo en los supuestos en que se acredite mala fe en su actuación.

Se entenderán nulas y sin efecto legal las decisiones del empleador tomadas en perjuicio o detrimento de los derechos laborales de los trabajadores que hayan actuado conforme a este apartado.

**Artículo 21.** *Factores para determinar la importancia de los efectos de un incidente.*

1. A los efectos de las notificaciones a las que se refiere el artículo 19.1, primer párrafo, la importancia de un incidente se determinará teniendo en cuenta, como mínimo, los siguientes factores:

a) El número de usuarios afectados por la perturbación del servicio esencial.
b) La duración del incidente.
c) La extensión o áreas geográficas afectadas por el incidente.
d) El grado de perturbación del funcionamiento del servicio.
e) El alcance del impacto en actividades económicas y sociales cruciales.
f) La importancia de los sistemas afectados o de la información afectada por el incidente para la prestación del servicio esencial.
g) El daño a la reputación.

2. En las notificaciones a las que se refiere el artículo 19.2, la importancia de un incidente se determinará conforme a lo que establezcan los actos de ejecución previstos en los apartados 8 y 9 del artículo 16 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016.

**Artículo 22.** *Notificación inicial, notificaciones intermedias y notificación final.*

1. Los operadores de servicios esenciales deberán realizar una primera notificación de los incidentes a los que se refiere el artículo 19.1 sin dilación indebida.

La notificación incluirá, entre otros datos, información que permita determinar cualquier efecto transfronterizo del incidente.

2. Los operadores de servicios esenciales efectuarán las notificaciones intermedias que sean precisas para actualizar la información incorporada a la notificación inicial e informar sobre la evolución del incidente, mientras éste no esté resuelto.

3. Los operadores de servicios esenciales enviarán una notificación final del incidente tras su resolución.

Un incidente se considerará resuelto cuando se hayan restablecido las redes y sistemas de información afectados y el servicio opere con normalidad.

**Artículo 23.** *Flexibilidad en la observancia de los plazos para la notificación.*

Los operadores de servicios esenciales y los proveedores de servicios digitales podrán omitir, en las comunicaciones que realicen sobre los incidentes que les afecten, la información de la que aún no dispongan relativa a su repercusión sobre servicios esenciales u otros servicios que dependan de ellos para su prestación, u otra información de la que no dispongan. Tan pronto como conozcan dicha información deberán remitirla a la autoridad competente.

Si, transcurrido un tiempo prudencial desde la notificación inicial del incidente, el operador de servicios esenciales o el proveedor de servicios digitales no hubiera podido reunir la información pertinente, enviará a la autoridad competente, sin demora, un informe justificativo de las actuaciones realizadas para reunir la información y de los motivos por los que no ha sido posible obtenerla.

**Artículo 24.** *Incidentes que afecten a servicios digitales.*

Los operadores de servicios esenciales y los proveedores de servicios digitales sometidos a este real decreto-ley, así como cualquier otra parte interesada, que tengan noticia de incidentes que afecten de modo significativo a servicios digitales ofrecidos en España por proveedores establecidos en otros Estados miembros de la Unión Europea, podrán notificarlo a la autoridad competente aportando la información pertinente, al objeto de facilitar la cooperación con el Estado miembro en el que estuviese establecido el citado proveedor.

Del mismo modo, si tienen noticia de que dichos proveedores han incumplido los requisitos de seguridad o de notificación de incidentes ocurridos en España que les son aplicables, podrán notificarlo a la autoridad competente aportando la información pertinente.

**Artículo 25.** *Tramitación de incidentes con impacto transfronterizo.*

1. Cuando las autoridades competentes o los CSIRT de referencia tengan noticia de incidentes que pueden afectar a otros Estados miembros de la Unión Europea, informarán a través del punto de contacto único a los Estados miembros afectados, precisando si el incidente puede tener efectos perturbadores significativos para los servicios esenciales prestados en dichos Estados.

2. Cuando a través de dicho punto de contacto se reciba información sobre incidentes notificados en otros países de la Unión Europea que puedan tener efectos perturbadores significativos para los servicios esenciales prestados en España, se remitirá la información relevante a la autoridad competente y al CSIRT de referencia, para que adopten las medidas pertinentes en el ejercicio de sus funciones respectivas.

3. Las actuaciones consideradas en los apartados anteriores se entienden sin perjuicio de los intercambios de información que las autoridades competentes o los CSIRT de referencia puedan realizar de modo directo con sus homólogos de otros Estados miembros de la Unión Europea en relación con aquellos incidentes que puedan resultar de interés mutuo.

**Artículo 26.** *Información al público.*

1. La autoridad competente podrá exigir a los operadores de servicios esenciales o a los proveedores de servicios digitales que informen al público o a terceros potencialmente interesados sobre los incidentes cuando su conocimiento sea necesario para evitar nuevos incidentes o gestionar uno que ya se haya producido, o cuando la divulgación de un incidente redunde en beneficio del interés público.

2. La autoridad competente también podrá decidir informar de modo directo al público o a terceros sobre el incidente.

En estos casos la autoridad competente consultará y se coordinará con el operador de servicios esenciales o el proveedor de servicios digitales antes de informar al público.

**Artículo 27.** *Información anual al punto de contacto único y al grupo de cooperación.*

1. Las autoridades competentes transmitirán al punto de contacto único un informe anual sobre el número y tipo de incidentes comunicados, sus efectos en los servicios prestados o en otros servicios y su carácter nacional o transfronterizo dentro de la Unión Europea.

Las autoridades competentes elaborarán el informe siguiendo las instrucciones que dicte el punto de contacto único teniendo en cuenta las indicaciones del grupo de cooperación respecto al formato y contenido de la información a transmitir.

2. El punto de contacto único remitirá al grupo de cooperación antes del 9 de agosto de cada año un informe anual resumido sobre las notificaciones recibidas, y lo remitirá ulteriormente a las autoridades competentes y a los CSIRT de referencia, para su conocimiento.

**Artículo 28.** *Obligación de resolver los incidentes, de información y de colaboración mutua.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales tienen la obligación de resolver los incidentes de seguridad que les afecten, y de solicitar ayuda especializada, incluida la del CSIRT de referencia, cuando no puedan resolver por sí mismos los incidentes.

En tales casos deberán atender a las indicaciones que reciban del CSIRT de referencia para resolver el incidente, mitigar sus efectos y reponer los sistemas afectados.

2. Los operadores de servicios esenciales y los proveedores de servicios digitales han de suministrar al CSIRT de referencia y a la autoridad competente toda la información que se les requiera para el desempeño de las funciones que les encomienda el presente real decreto-ley.

En particular, podrá requerirse información adicional a los operadores de servicios esenciales y a los proveedores de servicios digitales para analizar la naturaleza, causas y efectos de los incidentes notificados, y para elaborar estadísticas y reunir los datos necesarios para elaborar los informes anuales considerados en el artículo 27.

Cuando las circunstancias lo permitan, la autoridad competente o el CSIRT de referencia proporcionarán a los operadores de servicios esenciales o a los proveedores de servicios digitales afectados por incidentes la información derivada de su seguimiento que pueda serles relevante, en particular, para resolver el incidente.

**Artículo 29.** *Cooperación en lo relativo a los incidentes que afecten a datos personales.*

Las autoridades competentes y los CSIRT de referencia cooperarán estrechamente con la Agencia Española de Protección de Datos para hacer frente a los incidentes que den lugar a violaciones de datos personales.

Las autoridades competentes y los CSIRT de referencia comunicarán sin dilación a la Agencia Española de Protección de Datos los incidentes que puedan suponer una vulneración de datos personales y la mantendrán informada sobre la evolución de tales incidentes.

**Artículo 30.** *Autorización para la cesión de datos personales.*

Si la notificación de incidentes o su gestión, análisis o resolución requiriera comunicar datos personales, su tratamiento se restringirá a los que sean estrictamente adecuados, pertinentes y limitados a lo necesario en relación con la finalidad, de las indicadas, que se persiga en cada caso.

Su cesión para estos fines se entenderá autorizada en los siguientes casos:

a) De los operadores de servicios esenciales y los proveedores de servicios digitales a las autoridades competentes, a través de los CSIRT de referencia.

b) Entre los CSIRT de referencia y las autoridades competentes, y viceversa.

c) Entre los CSIRT de referencia, y entre éstos y los CSIRT designados en otros Estados miembros de la Unión Europea.

d) Entre los CSIRT de referencia y otros CSIRT nacionales o internacionales.

e) Entre el punto de contacto único y los puntos de contacto únicos de otros Estados miembros de la Unión Europea.

**Artículo 31.** *Notificaciones voluntarias.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales podrán notificar los incidentes para los que no se establezca una obligación de notificación.

Así mismo, las entidades que presten servicios esenciales y no hayan sido identificadas como operadores de servicios esenciales y que no sean proveedores de servicios digitales podrán notificar los incidentes que afecten a dichos servicios.

Estas notificaciones obligan a la entidad que las efectúe a resolver el incidente de acuerdo con lo establecido en el artículo 28.

2. Las notificaciones a las que se refiere el apartado anterior se regirán por lo dispuesto en este título, y se informará sobre ellas al punto de contacto único en el informe anual previsto en el artículo 27.1.

3. Las notificaciones obligatorias gozarán de prioridad sobre las voluntarias a los efectos de su gestión por los CSIRT y por las autoridades competentes.

## TÍTULO VI

## Supervisión

**Artículo 32.** *Supervisión de los operadores de servicios esenciales.*

1. Las autoridades competentes podrán requerir a los operadores de servicios esenciales para que les proporcionen toda la información necesaria para evaluar la seguridad de las redes y sistemas de información, incluida la documentación sobre políticas de seguridad.

Podrán requerirles información sobre la aplicación efectiva de su política de seguridad, así como auditar o exigir al operador que someta la seguridad de sus redes y sistemas de información a una auditoría por una entidad externa, solvente e independiente.

2. A la vista de la información recabada, la autoridad competente podrá requerir al operador que subsane las deficiencias detectadas e indicarle cómo debe hacerlo.

**Artículo 33.** *Supervisión de los proveedores de servicios digitales.*

1. La autoridad competente para la supervisión de los servicios digitales sólo inspeccionará el cumplimiento de las obligaciones derivadas de este real decreto-ley cuando tenga noticia de algún incumplimiento, incluyendo por petición razonada de otros órganos o denuncia.

En tal caso, la autoridad competente podrá requerir al proveedor de servicios digitales para que le proporcione toda la información necesaria para evaluar la seguridad de sus redes y sistemas de información, incluida la documentación sobre políticas de seguridad, y para que subsane las deficiencias detectadas.

2. Cuando la autoridad competente tenga noticia de incidentes que perturben de modo significativo a servicios digitales ofrecidos en otros Estados miembros por proveedores establecidos en España, adoptará las medidas de supervisión pertinentes.

A estos efectos, tendrá especialmente en cuenta la información facilitada por las autoridades competentes de otros Estados miembros.

**Artículo 34.** *Cooperación transfronteriza.*

1. La supervisión se llevará a cabo, cuando proceda, en cooperación con las autoridades competentes de los Estados miembros en los que se ubiquen las redes y sistemas de información empleados para la prestación del servicio, o en que esté establecido el operador de servicios esenciales, el proveedor de servicios digitales o su representante.

2. Las autoridades competentes colaborarán con las autoridades competentes de otros Estados miembros cuando éstas requieran su cooperación en la supervisión y adopción de medidas por operadores de servicios esenciales y proveedores de servicios digitales en relación con las redes y sistemas de información ubicados en España, así como respecto a los proveedores de servicios digitales establecidos en España o cuyo representante en la Unión Europea tenga su residencia o domicilio social en España.

## TÍTULO VII

## Régimen sancionador

**Artículo 35.** *Responsables.*

Serán responsables los operadores de servicios esenciales y los proveedores de servicios digitales comprendidos en el ámbito de aplicación de este real decreto-ley.

**Artículo 36.** *Infracciones.*

1. Las infracciones de los preceptos de este real decreto-ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) La falta de adopción de medidas para subsanar las deficiencias detectadas, de acuerdo con lo dispuesto en los artículos 32.2 o 33.1, cuando éstas le hayan hecho vulnerable a un incidente con efectos perturbadores significativos en el servicio y el operador de servicios esenciales o el proveedor de servicios digitales no hubiera atendido los requerimientos dictados por la autoridad competente con anterioridad a la producción del incidente.

b) El incumplimiento reiterado de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio. Se considerará que es reiterado a partir del segundo incumplimiento.

c) No tomar las medidas necesarias para resolver los incidentes con arreglo a lo dispuesto en el artículo 28.1 cuando éstos tengan un efecto perturbador significativo en la prestación servicios esenciales o de servicios digitales en España o en otros Estados miembros.

3. Son infracciones graves:

a) El incumplimiento de las disposiciones reglamentarias o de las instrucciones técnicas de seguridad dictadas por la autoridad competente referidas a las precauciones mínimas que los operadores de servicios esenciales han de adoptar para garantizar la seguridad de las redes y sistemas de información.

b) La falta de adopción de medidas para subsanar las deficiencias detectadas en respuesta a un requerimiento dictado de acuerdo con los artículos 32.2 o 33.1, cuando ese sea el tercer requerimiento desatendido que se dicta en los cinco últimos años.

c) El incumplimiento de la obligación de notificar incidentes con efectos perturbadores significativos en el servicio.

d) La demostración de una notoria falta de interés en la resolución de incidentes con efectos perturbadores significativos notificados cuando dé lugar a una mayor degradación del servicio.

e) Proporcionar información falsa o engañosa al público sobre los estándares que cumple o las certificaciones de seguridad que mantiene en vigor.

f) Poner obstáculos a la realización de auditorías por la autoridad competente.

4. Son infracciones leves:

a) El incumplimiento de las disposiciones reglamentarias o de las instrucciones técnicas de seguridad dictadas por la autoridad competente al amparo de este real decreto-ley, cuando no suponga una infracción grave.

b) La falta de adopción de medidas para corregir las deficiencias detectadas en respuesta a un requerimiento de subsanación dictado de acuerdo con los artículos 32.2 o 33.1.

c) No facilitar la información que sea requerida por las autoridades competentes sobre sus políticas de seguridad, o proporcionar información incompleta o tardía sin justificación.

d) No someterse a una auditoría de seguridad según lo ordenado por la autoridad competente.

e) No proporcionar al CSIRT de referencia o a la autoridad competente la información que soliciten en virtud del artículo 28.2.

f) La falta de notificación de los sucesos o incidencias para los que, aunque no hayan tenido un efecto adverso real sobre los servicios, exista obligación de notificación en virtud del párrafo segundo del artículo 19.2.

g) No completar la información que debe reunir la notificación de incidentes teniendo en cuenta lo dispuesto en el artículo 23, o no remitir el informe justificativo sobre la imposibilidad de reunir la información previsto en dicho artículo.

h) No seguir las indicaciones que reciba del CSIRT de referencia para resolver un incidente, de acuerdo con el artículo 28.

**Artículo 37.** *Sanciones.*

1. Por la comisión de las infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, multa de 500.001 hasta 1.000.000 euros.
b) Por la comisión de infracciones graves, multa de 100.001 hasta 500.000 euros.
c) Por la comisión de infracciones leves, amonestación o multa hasta 100.000 euros.

2. Las sanciones firmes en vía administrativa por infracciones muy graves y graves podrán ser publicadas, a costa del sancionado, en el «Boletín Oficial del Estado» y en el sitio de Internet de la autoridad competente, en atención a los hechos concurrentes y de conformidad con el artículo siguiente.

**Artículo 38.** *Graduación de la cuantía de las sanciones.*

El órgano sancionador establecerá la sanción teniendo en cuenta los siguientes criterios:

a) El grado de culpabilidad o la existencia de intencionalidad.
b) La continuidad o persistencia en la conducta infractora.
c) La naturaleza y cuantía de los perjuicios causados.

d) La reincidencia, por comisión en el último año de más de una infracción de la misma naturaleza, cuando así haya sido declarado por resolución firme en vía administrativa.

e) El número de usuarios afectados.

f) El volumen de facturación del responsable.

g) La utilización por el responsable de programas de recompensa por el descubrimiento de vulnerabilidades en sus redes y sistemas de información.

h) Las acciones realizadas por el responsable para paliar los efectos o consecuencias de la infracción.

**Artículo 39.** *Proporcionalidad de sanciones.*

1. El órgano sancionador podrá establecer la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate, en los siguientes supuestos:

a) Cuando se aprecie una cualificada disminución de la culpabilidad del imputado como consecuencia de la concurrencia significativa de varios de los criterios enunciados en el artículo 38.

b) Cuando la entidad infractora haya regularizado la situación irregular de forma diligente.

c) Cuando el infractor haya reconocido espontáneamente su culpabilidad.

2. Los órganos con competencia sancionadora, atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el apartado anterior, podrán no acordar el inicio del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que, en cada caso, resulten pertinentes, siempre que concurran los siguientes presupuestos:

a) Que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en este real decreto-ley.

b) Que el órgano competente no hubiese sancionado o apercibido al infractor en los dos años previos como consecuencia de la comisión de infracciones previstas en este real decreto-ley.

Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

3. No podrán ser objeto de apercibimiento las infracciones leves descritas en el artículo 36.4 c), d) y e) y la infracción grave prevista en el artículo 36.3 e).

**Artículo 40.** *Infracciones de las Administraciones públicas.*

1. Cuando las infracciones a que se refiere el artículo 36 fuesen cometidas por órganos o entidades de las Administraciones Públicas, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al órgano o entidad infractora y a los afectados, si los hubiera.

Además de lo anterior, el órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran.

2. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refiere el apartado anterior.

**Artículo 41.** *Competencia sancionadora.*

1. La imposición de sanciones corresponderá, en el caso de infracciones muy graves, al Ministro competente en virtud de lo dispuesto en el artículo 9, y en el caso de infracciones graves y leves al órgano de la autoridad competente que se determine mediante el reglamento de desarrollo de este real decreto-ley.

2. La potestad sancionadora se ejercerá con arreglo a los principios y al procedimiento previstos en las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de

las Administraciones Públicas, y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

3. El ejercicio de la potestad sancionadora se sujetará al procedimiento aplicable, con carácter general, a la actuación de las Administraciones públicas. No obstante, el plazo máximo de duración del procedimiento será de un año y el plazo de alegaciones no tendrá una duración inferior a un mes.

**Artículo 42.** *Concurrencia de infracciones.*

1. No procederá la imposición de sanciones según lo previsto en este real decreto-ley cuando los hechos constitutivos de infracción lo sean también de otra tipificada en la normativa sectorial a la que esté sujeto el prestador del servicio y exista identidad del bien jurídico protegido.

2. Cuando, como consecuencia de una actuación sancionadora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

**Disposición adicional primera.** *Relación inicial de servicios esenciales y operadores de servicios esenciales.*

La Comisión Nacional para la Protección de las Infraestructuras Críticas aprobará una primera lista de servicios esenciales dentro de los sectores incluidos en el ámbito de aplicación de este real decreto-ley e identificará a los operadores que los presten que deban sujetarse a este real decreto-ley en el siguiente orden:

a) Antes del 9 de noviembre de 2018: los servicios esenciales y los operadores correspondientes a los sectores estratégicos energía, transporte, salud, sistema financiero, agua, e infraestructuras digitales.

b) Antes del 9 de noviembre de 2019: los servicios esenciales y los operadores correspondientes al resto de los sectores estratégicos recogidos en el anexo de la Ley 8/2011, de 28 de abril.

**Disposición adicional segunda.** *Comunicaciones electrónicas y servicios de confianza.*

La aplicación de este real decreto-ley a los operadores de redes y servicios de comunicaciones electrónicas y de servicios electrónicos de confianza que sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril, no obstará a la aplicación de su normativa específica en materia de seguridad.

El Ministerio de Economía y Empresa, como órgano competente para la aplicación de dicha normativa, y el Ministerio del Interior actuarán de manera coordinada en el establecimiento de obligaciones que recaigan sobre los operadores críticos. Así mismo, mantendrán un intercambio fluido de información sobre incidentes que les afecten.

**Disposición adicional tercera.** *Notificación de violaciones de seguridad de los datos personales a través de la plataforma común prevista en este real decreto-ley.*

La plataforma común para la notificación de incidentes prevista en este real decreto-ley podrá ser empleada para la notificación de vulneraciones de la seguridad de datos personales según el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en los términos que acuerden la Agencia Española de Protección de Datos y los órganos que gestionen dicha plataforma.

**Disposición adicional cuarta.** *Proveedores de servicios digitales ya existentes.*

Los proveedores de servicios digitales que ya vinieran prestando servicios deberán comunicar su actividad a la Secretaría de Estado para el Avance Digital del Ministerio de Economía y Empresa, en el plazo de tres meses desde la entrada en vigor de este real decreto-ley.

**Disposición final primera.** *Título competencial.*

Este real decreto-ley se dicta en virtud de las competencias exclusivas atribuidas al Estado en materia de régimen general de telecomunicaciones y seguridad pública, por el artículo 149.1.21.ª y 29.ª de la Constitución.

**Disposición final segunda.** *Incorporación del Derecho de la Unión Europea.*

Este real decreto-ley incorpora al ordenamiento jurídico interno la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

**Disposición final tercera.** *Habilitación para el desarrollo reglamentario.*

Se habilita al Gobierno para desarrollar reglamentariamente lo previsto en este real decreto-ley sin perjuicio de la competencia de los Ministros para fijar las obligaciones específicas mediante Orden Ministerial en los supuestos previstos en el articulado de esta norma.

**Disposición final cuarta.** *Entrada en vigor.*

El presente real decreto-ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

# § 35

## Orden PRE/2740/2007, de 19 de septiembre, por la que se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información

Ministerio de la Presidencia
«BOE» núm. 230, de 25 de septiembre de 2007
Última modificación: sin modificaciones
Referencia: BOE-A-2007-16830

La utilización de las Tecnologías de la Información (TI) en amplias áreas de la actividad de la Administración, así como la creciente participación de España en proyectos de desarrollo de la sociedad de la información de carácter internacional, imponen la necesidad de garantizar un nivel de seguridad en la utilización de las TI equiparable, como mínimo, al conseguido en el tratamiento tradicional de la información en soporte papel.

Por tanto, la seguridad que las TI deben poseer, ha de abarcar la protección de la confidencialidad, la integridad y la disponibilidad de la información que manejan los sistemas de información, así como la integridad y disponibilidad de los propios sistemas.

La garantía de seguridad de las Tecnologías de la Información debe estar basada en el establecimiento de mecanismos y servicios de seguridad, adecuadamente diseñados, que impidan la realización de funciones no deseadas.

Uno de los métodos, admitido internacionalmente, para garantizar la corrección y efectividad de dichos mecanismos y servicios, consiste en la evaluación de la seguridad de las TI, realizada mediante la utilización de criterios rigurosos, con posterior certificación por el organismo legalmente establecido.

El Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, que acompaña a esta Orden Ministerial, regula el marco de actuación, y crea los organismos necesarios, para poner estos procesos de evaluación y certificación al alcance de la industria y de la Administración; todo ello basado en el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

La carencia actual de un esquema análogo, puede suponer un importante obstáculo para la difusión y aceptación generalizada, tanto a nivel nacional como internacional, de los diferentes productos y sistemas de las Tecnologías de la Información desarrollados en nuestro país.

En el contexto de los programas internacionales, no se puede entender criterios de evaluación y certificación de la seguridad de las TI que no sean homologables con los de otros países participantes. Por ello, es necesario la adopción de criterios internacionales, que permitan negociar el reconocimiento mutuo de certificados, resultando esencial que el Esquema al que se refiere el presente Reglamento, se equipare a los del resto de los países de nuestro entorno.

Desde hace algunos años, en España, se ha venido sintiendo la necesidad de impulsar la creación de un esquema de esta naturaleza, habiéndose llevado a cabo diversas

iniciativas para su constitución, desde el Consejo Superior de Informática y para el Impulso de la Administración Electrónica, en colaboración con el Centro Nacional de Inteligencia. También, en la Dirección General de Armamento y Material del Ministerio de Defensa, se creó un esquema orientado a satisfacer necesidades puntuales del Ministerio de Defensa.

Asimismo, se creó un laboratorio de evaluación, el Centro de Evaluación de la Seguridad de las Tecnologías de la Información (CESTI) del Instituto Nacional de Técnica Aeroespacial (INTA). Este laboratorio fue acreditado, siguiendo este mismo Reglamento, como laboratorio de evaluación de la seguridad de las Tecnologías de la Información, por resolución 1AO/38272/2005, de 13 de octubre, del Centro Criptológico Nacional, y ha contribuido, de manera decisiva, a la creación y puesta en marcha de un esquema de funcionalidad completa.

Paralelamente, España, como país consumidor de certificados, y a través del Ministerio de Administraciones Públicas, ha estado presente en el Arreglo de Reconocimiento Mutuo de Certificados Common Criteria (CCRA), desde su creación.

En ese Ministerio, se ha sentido la necesidad de crear un único esquema nacional que abarcase todo el ámbito de la actividad de evaluación y certificación y que potenciase a España a la categoría de país productor de certificados Common Criteria.

Por todo ello, la creación de un esquema nacional va a gozar, desde el principio, de aportaciones experimentadas y se va a encajar en un foro en el que su presencia es demandada.

Por otra parte, se hace necesaria la participación de un organismo de certificación, que partiendo de un conocimiento de las Tecnologías de la Información y de las amenazas y vulnerabilidades existentes, proporcione una garantía razonable a los procesos de evaluación y certificación.

Dicho organismo se constituye al amparo de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, que encomienda a este Centro el ejercicio de las funciones relativas a la seguridad de las Tecnologías de la Información, y según lo dispuesto en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, entre cuyas funciones está la de constituir el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

En virtud de los preceptos indicados anteriormente, consultados los fabricantes e importadores del sector, y a propuesta conjunta de los Ministros de Defensa y de Industria, Turismo y Comercio, con la aprobación previa de la Ministra de Administraciones Públicas, dispongo:

**Artículo único.** *Aprobación del Reglamento.*

Se aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información, cuyo texto se inserta a continuación.

**Disposición adicional única.** *Naturaleza y establecimiento de la contraprestación exigida por las acreditaciones y certificaciones.*

1. Al amparo de lo dispuesto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, los ingresos procedentes de las acreditaciones de laboratorios y de las certificaciones de productos, tienen la naturaleza de tasas.

2. Según lo establecido en el artículo 2.3 del Real Decreto 1287/2005, de 28 de octubre, por el que se modifica el Real Decreto 593/2002, de 28 de junio, que desarrolla el régimen económico presupuestario del Centro Nacional de Inteligencia, el establecimiento o modificación de la cuantía de los ingresos que tengan la naturaleza de tasas, así como la fijación de los diversos elementos de la correspondiente relación jurídico-tributaria, se harán con arreglo a lo dispuesto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos.

**Disposición final primera.** *Facultades de ejecución y aplicación.*

Se faculta al Secretario de Estado Director del Centro Criptológico Nacional del Centro Nacional de Inteligencia, para dictar cuantas instrucciones sean necesarias para la ejecución y aplicación de lo establecido en esta orden ministerial.

**Disposición final segunda.** *Entrada en vigor.*

La presente orden ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## REGLAMENTO DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

### CAPÍTULO I

### Disposiciones generales

**Artículo 1.** *Objeto.*

El presente Reglamento tiene por objeto la articulación del Organismo de Certificación (OC) del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) en el ámbito de actuación del Centro Criptológico Nacional, según lo dispuesto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, respectivamente.

**Artículo 2.** *Definiciones.*

En el marco del presente Reglamento, los conceptos que a continuación se indican, se entenderán como están definidos.

Acreditación.–Declaración de conformidad de los laboratorios solicitantes, emitida por el Organismo de Certificación, en base al cumplimiento de los requisitos establecidos en el Capítulo III, y según el procedimiento establecido en el Capítulo IV, del presente Reglamento.

Acreditación de competencia técnica.–Es aquella acreditación que concede una entidad de acreditación reconocida a un laboratorio, conforme a lo regulado en la Ley 21/1992, de 16 de julio, de Industria y en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la infraestructura para la calidad y seguridad industrial, y en base al cumplimiento, por parte del laboratorio, de la norma UNE-EN ISO/IEC 17025. En su alcance se deberán incluir las normas de evaluación de la seguridad de los productos y sistemas de Tecnologías de la Información aprobadas por el Organismo de Certificación.

Certificación.–Es la determinación, obtenida mediante un proceso metodológico de evaluación, de la conformidad de un producto con unos criterios preestablecidos.

Declaración de seguridad.–Conjunto de requisitos y especificaciones de las propiedades de seguridad de un producto o sistema de las Tecnologías de la Información.

Evaluación.–Es el análisis, realizado mediante un proceso metodológico, de la capacidad de un producto o sistema de las Tecnologías de la Información para proteger las condiciones de la información de acuerdo a unos criterios establecidos, con objeto de determinar si puede ser certificado.

Información de las evaluaciones.–Es todo asunto, acto, documento, dato u objeto relacionado con la actividad de evaluación de la seguridad de un producto. La información de las evaluaciones incluye toda la documentación, programas de ordenador, esquemas, planos y demás datos suministrados por el fabricante, los programas de ordenador, planes, pruebas, análisis y resultados de la evaluación elaborados por el laboratorio, así como toda la documentación administrativa y contractual y las comunicaciones del laboratorio con el fabricante del producto y con el Organismo de Certificación, además de los registros de la actividad del laboratorio, incluyendo los de seguridad.

Producto a evaluar.–Es el producto, sistema de información o perfil de protección para el que se solicita una certificación de sus propiedades de seguridad.

Producto clasificado.–Son aquellos productos con requisitos específicos para manejar con seguridad materias clasificadas, o cuya información de especificación, diseño o desarrollo está clasificada, incluso parcialmente, según lo dispuesto en la Ley 9/68, de 5 de abril, sobre Secretos Oficiales, modificada por la Ley 48/78, de 7 de octubre.

Laboratorio de evaluación.–Es un laboratorio de ensayo, según se define en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la infraestructura para la calidad y seguridad industrial.

Sistema de información.–Es el conjunto de elementos «hardware», «software», datos y usuarios que, relacionados entre sí, permiten el almacenamiento, transmisión, transformación y recuperación de la información.

**Artículo 3.** *Ámbito de aplicación.*

El ámbito de actuación del Organismo de Certificación comprende las entidades públicas o privadas que quieran ejercer de laboratorios de evaluación de la seguridad de las TI en el marco del Esquema.

También comprende a estas entidades cuando sean fabricantes de productos o sistemas de TI que quieran certificar la seguridad de dichos productos, en el marco del Esquema.

Todo ello, siempre que dichos productos o sistemas sean susceptibles de ser incluidos en el ámbito de actuación del Centro Criptológico Nacional.

## CAPÍTULO II

## Estructura y funciones del organismo de certificación

### *Sección 1.ª Estructura del organismo de certificación*

**Artículo 4.** *Estructura.*

A los efectos de funcionamiento del Organismo de Certificación, su estructura será la siguiente:

a) Director del Organismo de Certificación, que será el Secretario de Estado Director del Centro Criptológico Nacional.

b) Secretario General del Organismo de Certificación, que será el Secretario General del Centro Criptológico Nacional.

c) Subdirector de Certificación, que será un funcionario del Centro Nacional de Inteligencia, con rango de Subdirector General, designado por el Director del Organismo de Certificación.

d) Jefe del Área de Certificación, que será un funcionario del Centro Criptológico Nacional, con rango de Subdirector General Adjunto, designado por el Subdirector de Certificación.

e) Los correspondientes Responsables, Técnico de Certificación, de Calidad, de Seguridad, y de Registro, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.

f) Personal técnico de certificación, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.

g) Personal de enlace con los servicios de Secretaría, y demás personal de soporte administrativo a las actividades del Organismo de Certificación, que serán funcionarios del Centro Criptológico Nacional designados por el Jefe del Área de Certificación.

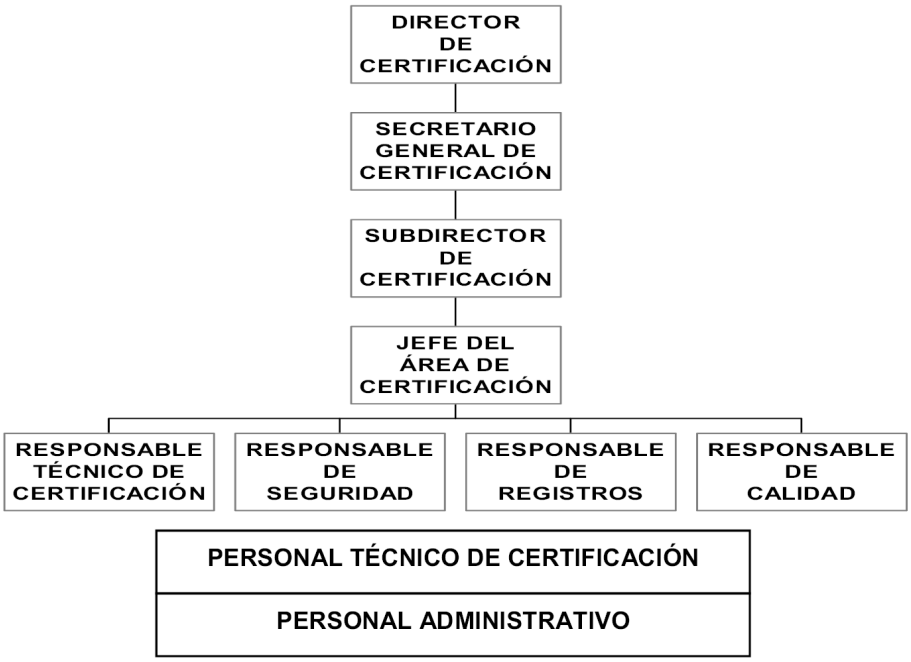



Figura 1. Estructura del Organismo de Certificación

***Sección 2.ª Funciones de los cargos del organismo de certificación***

**Artículo 5.** *Director del Organismo de Certificación.*

Corresponde al Director del Organismo de Certificación:

a) Aprobar y hacer cumplir las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación, garantizando la adecuación de la organización y de los medios materiales y humanos a los fines propuestos.

b) Dictar las resoluciones sobre las solicitudes de acreditación de laboratorios y de certificación de la seguridad de productos y sistemas de las Tecnologías de la Información.

c) Establecer los acuerdos oportunos con otros organismos similares en el ámbito de su competencia.

**Artículo 6.** *Secretario General del Organismo de Certificación.*

Corresponde al Secretario General del Organismo de Certificación:

a) Apoyar y asistir al Director del Organismo de Certificación en el ejercicio de sus funciones.

b) Establecer los mecanismos y sistemas de organización del Organismo de Certificación y determinar las actuaciones precisas para su actualización y mejora.

c) Dirigir el funcionamiento de los servicios comunes del Organismo de Certificación a través de las correspondientes instrucciones y órdenes de servicio.

d) Desempeñar la jefatura superior del personal del Organismo de Certificación, elaborar la propuesta de relación de puestos de trabajo y determinar los puestos vacantes a proveer durante cada ejercicio.

**Artículo 7.** *Subdirector de Certificación.*

Corresponde al Subdirector de Certificación:

a) Presidir el Consejo de Acreditación y Certificación, conforme a lo establecido en el presente Reglamento.

b) Representar al Organismo de Certificación en aquellos foros de índole técnica, de normalización y de divulgación de las actividades del citado organismo, de las normas aplicables y en los de arreglos y acuerdos de reconocimiento mutuo.

c) Revisar las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación.

d) Proponer los presupuestos y planes de formación anuales del Organismo de Certificación.

**Artículo 8.** *Jefe del Área de Certificación.*

Corresponde al Jefe del Área de Certificación:

a) Desempeñar la dirección de los servicios técnicos del Organismo de Certificación.

b) Dirigir las instrucciones y procedimientos de acreditación de laboratorios y de certificación de productos.

c) Elevar las correspondientes propuestas de resolución a las mencionadas solicitudes de acreditación y certificación.

d) Instruir, de oficio, los procedimientos de mantenimiento de la acreditación de los laboratorios.

**Artículo 9.** *Responsable Técnico de Certificación.*

Corresponde al Responsable Técnico de Certificación:

a) Apoyar y asistir al Jefe del Área de Certificación en el ejercicio de sus funciones.

b) Coordinar y dirigir la actuación diaria del personal técnico del Organismo de Certificación.

c) Realizar la asignación de personal técnico a la instrucción de cada solicitud de acreditación de laboratorio y de certificación de producto.

d) Dictaminar las interpretaciones técnicas de normas, métodos y procedimientos de evaluación empleados, bien de oficio, o a instancia de los laboratorios.

e) Elaborar o proponer las políticas, manuales y procedimientos que regulan la actuación del Organismo de Certificación.

**Artículo 10.** *Responsable de Calidad del Organismo de Certificación.*

Corresponde al Responsable de Calidad del Organismo de Certificación:

a) Garantizar y auditar la ejecución del sistema de gestión de la calidad del Organismo de Certificación, con las funciones específicas en él indicadas.

b) Proponer, al Jefe del Área de Certificación, las mejoras convenientes para la eficacia del sistema de gestión de calidad, tras su evaluación.

**Artículo 11.** *Responsable de Seguridad del Organismo de Certificación.*

Corresponde al Responsable de Seguridad del Organismo de Certificación:

a) Garantizar y auditar la ejecución del sistema de gestión de la seguridad del Organismo de Certificación, con las funciones específicas en él indicadas.

b) Proponer, al Jefe del Área de Certificación, las mejoras convenientes para la eficacia del sistema de gestión de la seguridad, tras su evaluación.

**Artículo 12.** *Responsable de Registro del Organismo de Certificación.*

Corresponde al Responsable de Registro del Organismo de Certificación, la gestión y custodia de los registros de calidad, seguridad, certificación y acreditación, manejados por el Organismo de Certificación.

**Artículo 13.** *Personal técnico del Organismo de Certificación.*

Corresponde al personal técnico del Organismo de Certificación, el desarrollo de la instrucción de los expedientes de acreditación de laboratorio y de certificación de productos,

practicando las pruebas conforme a los medios y procedimientos establecidos por el Organismo de Certificación.

***Sección 3.ª Consejo de acreditación y certificación***

**Artículo 14.** *Naturaleza.*

El Consejo de Acreditación y Certificación es un órgano colegiado, distinto e independiente del Organismo de Certificación, regido por lo establecido en el Capítulo II del Título II, de la Ley 30/92, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y, por lo establecido en el presente Reglamento.

**Artículo 15.** *Composición.*

Corresponde al Subdirector de Certificación la presidencia del Consejo de Acreditación y Certificación.

Formarán parte como miembros del Consejo, los siguientes:

a) El Jefe del Área de Certificación, que podrá asumir la presidencia del Consejo por delegación del Subdirector de Certificación.

b) El Responsable Técnico de Certificación, que hará las veces de Secretario del Consejo.

c) Un representante del Ministerio de Defensa, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Ministerio.

d) Un representante del Ministerio de Industria, Turismo y Comercio, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Ministerio.

e) Un representante del Consejo Superior de Administración Electrónica, cuyo nombramiento y asistencia solicitará el Organismo de Certificación a dicho Consejo.

f) Un representante de cada laboratorio acreditado, nombrado por dicho laboratorio.

g) Dos representantes de los sectores empresariales de fabricantes, importadores e integradores de productos y sistemas de las Tecnologías de la Información, a propuesta razonada y acordada de dichos sectores.

**Artículo 16.** *Fines.*

Corresponde al Consejo de Acreditación y Certificación:

a) Vigilar que la normativa del Organismo de Certificación se corresponda y equipare con los términos y referencias de esquemas de certificación equivalentes, que pudieran existir en el ámbito de la Unión Europea en particular, y en el ámbito internacional, en general.

b) Asesorar al Organismo de Certificación en la evolución de sus procedimientos documentados, orientando la gestión de éste, al mejor servicio del tejido industrial y empresarial de fabricantes, importadores e integradores de productos y sistemas de Tecnologías de la Información.

c) Asesorar al Organismo de Certificación en la identificación de esquemas, arreglos o acuerdos, donde la defensa de la validez y reconocimiento mutuo de los certificados emitidos sea de interés para la Administración y el sector privado español.

**Artículo 17.** *Atribuciones.*

Las atribuciones del Consejo de Acreditación y Certificación son las siguientes:

a) Estar permanentemente informado de la normativa que regula el funcionamiento del Organismo de Certificación, incluyendo sus normas de evaluación y certificación, manuales, procedimientos e instrucciones técnicas.

b) Estar permanentemente informado de la relación de laboratorios acreditados y de productos certificados.

c) Estar permanentemente informado de la relación de esquemas de certificación de la seguridad de los productos y sistemas de información, con los que el Organismo de

Certificación tiene establecidos arreglos o acuerdos de reconocimiento mutuo de certificados.

d) Proponer directrices y recomendaciones al Organismo de Certificación, que serán recogidas en las correspondientes actas de las reuniones del Consejo, a las que deberá dar cumplida respuesta el Director del Organismo de Certificación.

**Artículo 18.** *Periodicidad de las reuniones.*

El Consejo de Acreditación y Certificación se reunirá, como mínimo, una vez al año, sin perjuicio de que en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.

Las reuniones se convocarán a requerimiento del Organismo de Certificación, o por acuerdo del propio Consejo de Acreditación.

### *Sección 4.ª Acreditación y certificación*

**Artículo 19.** *Acreditación de laboratorios.*

El Organismo de Certificación acredita a los laboratorios solicitantes, en base al cumplimiento de los requisitos establecidos en el Capítulo III, y según el procedimiento establecido en el Capítulo IV de este Reglamento.

**Artículo 20.** *Certificación de productos.*

El Organismo de Certificación certifica la seguridad de los productos y sistemas de Tecnologías de la Información, según lo establecido en el procedimiento del Capítulo V, y atendiendo a los criterios, métodos y normas de evaluación de la seguridad, establecidos en el Capítulo VI.

**Artículo 21.** *Publicaciones del Esquema.*

El Organismo de Certificación mantendrá actualizada la relación de laboratorios acreditados y la de productos y sistemas de las Tecnologías de la Información certificados. Dicha relación se podrá consultar en la siguiente dirección electrónica: http://www.oc.ccn.cni.es.

## CAPÍTULO III

## Requisitos de acreditación de laboratorios

**Artículo 22.** *Requisitos generales para la acreditación de laboratorios.*

1. Para la acreditación de los laboratorios de evaluación de la seguridad de las Tecnologías de la Información se requerirá el cumplimiento de los siguientes requisitos:

a) Capacidad para la evaluación de la seguridad de productos de las Tecnologías de la Información, demostrada mediante la acreditación de la competencia técnica en vigor, conforme a la norma UNE-EN ISO/IEC 17025, cuyo alcance incluya los criterios, métodos y normas de evaluación recogidos en el Capítulo VI.

b) Cumplimiento de los requisitos de seguridad establecidos en la Sección 1.ª o en la Sección 2.ª de este Capítulo, según corresponda.

c) Desarrollo de las evaluaciones de acuerdo a procedimientos que recojan las obligaciones de información y coordinación con el Organismo de Certificación, indicadas en la Sección 3.ª de este mismo Capítulo.

2. La comprobación del cumplimiento de estos requisitos se realizará mediante el procedimiento de auditoría y seguimiento indicado en las Secciones 4.ª y 5.ª del Capítulo IV.

En todo caso, el alcance de la acreditación, otorgada por el Organismo de Certificación, estará limitado por el alcance de la acreditación de la competencia técnica del laboratorio, y cualificado por el nivel de seguridad del mismo.

3. Salvo en los casos en que haya una compartimentación organizativa, de medios y de procedimientos, aprobada por el Organismo de Certificación, el laboratorio deberá cumplir

con los requisitos de gestión de seguridad, necesarios para la acreditación, incluso en el desarrollo de aquellas evaluaciones cuyo objeto final no sea la certificación del producto evaluado por parte del Organismo de Certificación.

### *Sección 1.ª Requisitos de seguridad para laboratorios que evalúen productos clasificados*

**Artículo 23.** *Requisitos de laboratorios que evalúen productos clasificados.*

Los laboratorios, tanto de titularidad pública como privada, que pretendan evaluar productos clasificados deberán cumplir, además de los requisitos establecidos para los laboratorios que evalúen productos no clasificados, lo dispuesto en la Orden Ministerial Comunicada 17/2001, de 29 de enero, por la que se aprueba el Manual de Protección de Materias Clasificadas del Ministerio de Defensa en poder de las empresas.

Asimismo, deberán tener suscrito, y en vigor, Acuerdo de Seguridad, con un grado de calificación de seguridad igual o superior al grado de calificación de seguridad de la información del producto a evaluar.

### *Sección 2.ª Requisitos de seguridad para laboratorios que evalúen productos no clasificados*

**Artículo 24.** *Requisitos de laboratorios que evalúen productos no clasificados.*

Los laboratorios, tanto de titularidad pública como privada, que evalúen productos no clasificados, cumplirán con los requisitos de gestión de la seguridad, aplicables a la información de las evaluaciones, establecidos en esta Sección.

#### Subsección 1.ª Responsabilidades del laboratorio

**Artículo 25.** *Derecho de acceso a la información de las evaluaciones.*

El laboratorio facilitará al Organismo de Certificación el acceso a toda la información de las evaluaciones que lleve a cabo.

El laboratorio deberá obtener, del Organismo de Certificación, autorización escrita antes de permitir a terceros, incluido el fabricante del producto evaluado, cualquier tipo de acceso a la información de las evaluaciones, tales como, planes, pruebas, análisis y resultados de la evaluación.

El Organismo de Certificación podrá prohibir la difusión de determinada información originada por el laboratorio.

**Artículo 26.** *Plan de protección.*

1. El laboratorio deberá elaborar, poner en práctica y mantener al día un Plan de Protección de la Información de las evaluaciones.

2. Este plan incluirá, al menos, la siguiente información:

a) Una descripción del laboratorio, con indicación expresa de la ubicación, actividades empresariales distintas a las de evaluación, en su caso, organigrama, recursos humanos, factorías, sucursales y dependencias autónomas, incluyendo un plano con leyenda de las instalaciones del laboratorio.

b) Los fundamentos del Plan, que deberán comprender los objetivos concretos que han de alcanzarse con el mismo y que estarán dirigidos a prevenir, detectar y rehabilitar el daño causado por la manifestación del riesgo, así como la identificación de los riesgos contra los que se pretende la protección.

La confidencialidad, integridad y disponibilidad de la información de las evaluaciones serán del máximo interés para el Organismo de Certificación.

c) La descripción de la organización, donde se debe documentar la estructura de seguridad del laboratorio, la matriz de responsabilidades donde se establece la identificación exacta de los responsables en lo referente a la toma de decisiones, y la definición detallada de las misiones de cada componente del sistema, así como la coordinación del apoyo

potencial de organismo exteriores, tales como empresas de seguridad privada, centrales receptoras de alarmas, servicios de custodia de información, etc.

d) La descripción de las medidas de protección física, y el establecimiento de zonas de acceso restringido en las distintas dependencias del laboratorio.

e) Los Procedimientos Operativos de seguridad.

f) La descripción de las reacciones específicas a cada incidente de seguridad, desarrollando la matriz de responsabilidades en los cometidos y misiones que este plan asigne a la dirección del laboratorio, a los que formen parte del Servicio de Protección del laboratorio y al resto de personal, en lo que respecta a decisiones y actuaciones ante los riesgos de seguridad que se manifiesten y que se hayan considerado.

g) Los requisitos específicos de seguridad y los Procedimientos Operativos de seguridad de los sistemas de información del laboratorio.

**Artículo 27.** *Procedimientos Operativos de seguridad.*

1. Los Procedimientos Operativos de seguridad incluirán, en forma de directivas, los detalles específicos de actuación encaminados a la prevención de riesgos.

2. Estas actuaciones se deben corresponder con la matriz de responsabilidades, tratando de forma concreta y específica los siguientes aspectos, relativos a requisitos de seguridad establecidos por las condiciones de acreditación del laboratorio:

a) Las normas para el manejo y custodia de la información de las evaluaciones.

b) El tratamiento de las visitas, verificando periódicamente la eficacia del control de visitas al laboratorio, así como el correcto uso del libro de visitas o sistema alternativo.

c) La entrada en las zonas de acceso restringido.

d) El acceso, transmisión, reproducción, archivo y destrucción de información de las evaluaciones, con el establecimiento de los mecanismos necesarios que permitan identificar, en todo momento, al responsable de la tenencia de la información.

e) La regulación de las necesarias comprobaciones de seguridad, tanto durante la jornada de trabajo como al término de la misma.

f) La descripción del sistema de control de llaves.

g) El establecimiento del sistema de recibo interno, para control de información de las evaluaciones.

h) La operativa de actuación ante una incidencia de la central receptora de alarmas.

i) Los procedimientos de actuación de los vigilantes de seguridad.

**Artículo 28.** *Personal del laboratorio.*

El laboratorio deberá mantener actualizado un registro de seguridad de todo el personal afecto al mismo.

El laboratorio regulará, en base a la necesidad de conocer, el acceso de dicho personal a la información de las evaluaciones. Las autorizaciones de acceso a la información de las evaluaciones se comunicarán y revocarán por escrito, adjuntándose dichas comunicaciones al registro de seguridad del personal.

**Artículo 29.** *Comunicaciones preceptivas al Organismo de Certificación.*

El laboratorio deberá informar al Organismo de Certificación, en el plazo más breve posible, de lo siguiente:

a) Sobre toda información que llegue a su conocimiento en relación con accesos, o intentos de acceso, no autorizados a información de las evaluaciones; actos de sabotaje, o actividades que supongan un riesgo para dicha información.

b) Sobre toda anomalía, extravío, robo o manipulación relacionada con la información de las evaluaciones.

c) Sobre la presunción de que una transmisión de información de las evaluaciones haya sufrido vulneración o retraso injustificado.

d) Sobre las modificaciones que pretenda realizar en las zonas de acceso restringido.

e) Sobre las visitas que reciba conforme a lo que se expresa en la Subsección 5.ª, presente Capítulo y Sección.

f) Sobre las modificaciones del Plan de Protección, así como de las altas y bajas de personal y sobre la composición y cambios del Servicio de Protección.

**Artículo 30.** *Relaciones del laboratorio con contratistas.*

Los requisitos de seguridad requeridos por la acreditación del laboratorio, son también de aplicación a los contratistas del mismo que vayan a acceder a información de las evaluaciones.

El laboratorio deberá obtener, del Organismo de Certificación, autorización escrita antes de proporcionar al contratista el acceso a información de las evaluaciones. En su solicitud, comunicará los datos de identificación del contratista, así como la información de las evaluaciones a las que pudiera tener acceso, y el objeto y condiciones específicas de dicho acceso.

Como norma general, para la concesión de la autorización de acceso, el contratista deberá demostrar el cumplimiento de los requisitos de seguridad establecidos en el presente Reglamento mediante auditoría del Organismo de Certificación, conforme al procedimiento establecido en el Capítulo IV, salvo en los casos en que el Organismo de Certificación determine la aplicación de condiciones o limitaciones particulares a dicho acceso.

Subsección 2.ª Tratamiento de la información de las evaluaciones

**Artículo 31.** *Distintivos.*

1. Toda información de las evaluaciones llevará, de forma clara y visible, un signo distintivo de tal condición, que indicará la evaluación a la que corresponde.

2. Si se trata de documentos sueltos, se pondrá el signo distintivo en la parte superior e inferior de cada una de las páginas, centrado en las mismas, de tal forma que no pueda quedar oculto por dobleces, grapas, cubiertas, etc.

3. Si se trata de documentos permanentemente unidos o encuadernados, se pondrá el mencionado distintivo en la cubierta anterior y posterior, así como en todas sus páginas, conforme a lo indicado anteriormente.

4. Si se trata de planos, diagramas, esquemas o documentos similares, dicho distintivo se situará en la carátula y en la parte que identifique el documento.

5. Los soportes y sistemas informáticos que contengan o procesen información de las evaluaciones, se marcarán con los distintivos apropiados, para lo cual podrán emplearse etiquetas o cintas adhesivas.

6. Se seguirán procedimientos análogos para la protección de la información de las evaluaciones soportada en cualquier elemento, o conjunto de elementos, físicamente separables.

**Artículo 32.** *Libro registro de información de las evaluaciones.*

1. En cada dependencia del laboratorio donde se custodie información de las evaluaciones, existirá un registro donde figurará toda la información de las evaluaciones que haya tenido entrada o salida, las reproducciones y destrucciones, así como el acceso a dicha información por personal, tanto propio, como ajeno al laboratorio, con independencia de si esta información se almacena o transmite en papel o en soporte electrónico.

2. El registro se podrá mantener en soporte informático, en soporte papel (en forma de libro) o en una combinación de ambos soportes.

3. Estos registros deberán ser custodiados con la debida protección electrónica, si están en soporte informático, o en los muebles de seguridad ubicados en la zona de acceso restringido, si están en soporte papel.

4. El laboratorio deberá implementar los mecanismos correspondientes para que el registro de entrada/salida mediante soporte electrónico no se pueda eludir por el personal del mismo.

**Artículo 33.** *Recepción y recibo de la información de las evaluaciones.*

Cuando se reciba cualquier información de las evaluaciones, se seguirá el siguiente proceso:

a) Se examinará el envío para asegurarse de que no ha sido violado, comprobándose el contenido contra recibo. La evidencia de violación y las anomalías que se observen en el contenido deberán notificarse, cuanto antes, al remitente y al Organismo de Certificación.

b) Cuando el envío esté en orden, se firmará el recibo y se devolverá debidamente cumplimentado al remitente, realizando de manera inmediata la anotación en el libro registro.

**Artículo 34.** *Transmisión de la información de las evaluaciones.*

1. Se entiende por transmisión de la información de las evaluaciones, su traslado, comunicación, envío, entrega o divulgación a terceros.

2. Será necesario que la transmisión y custodia de la información de las evaluaciones sea controlada por un sistema de recibos, incluso dentro de las dependencias del laboratorio, con el fin de identificar, en cualquier momento, al responsable de su tenencia.

3. Cuando se trate de transmisión no electrónica de información de las evaluaciones, se realizará de la siguiente forma:

a) Por entrega directa del personal del laboratorio.

b) Por correo certificado nacional.

c) Por transportistas comerciales.

d) El embalaje de la información se llevará a cabo de forma que se pueda detectar su apertura; con cubiertas opacas que impidan desvelar su contenido, de tal naturaleza y resistencia, que aseguren su integridad durante el transporte; y, dicho embalaje, no tendrá ninguna indicación externa de la información contenida.

4. Cuando se trate de transmisión electrónica de información de las evaluaciones, se realizará utilizando las medidas técnicas y operacionales de protección de su confidencialidad que determine, en cada caso, el Organismo de Certificación.

**Artículo 35.** *Reproducción de la información de las evaluaciones.*

1. El número de reproducciones de la información de las evaluaciones, será el mínimo imprescindible. Se controlará mediante una correlativa numeración, que se recogerá en el registro, como anotación suplementaria del correspondiente original, indicando todos los datos referentes a dichas reproducciones y a la situación de cada una de ellas.

2. Cada reproducción, total o parcial, de información de las evaluaciones deberá ser numerada y tratada, a todos los efectos, como el original.

3. La reproducción de información de las evaluaciones deberá realizarse directamente por el laboratorio, sin recurrir a contratistas de artes gráficas. Se deberá comprobar, después de realizar las reproducciones, que en el mecanismo de reproducción no queda registro de la información reproducida.

**Artículo 36.** *Custodia y destrucción de la información de las evaluaciones.*

1. El laboratorio custodiará, por un plazo mínimo de cinco años, toda la información de cada evaluación, a contar desde la fecha de emisión del certificado correspondiente, o de la emisión del último informe técnico de evaluación, en el caso de productos no certificados.

2. En el caso de reevaluaciones, mantenimiento o extensiones del certificado, el cómputo de cinco años se referirá siempre al último certificado o informe técnico de evaluación aplicable.

3. Pasado dicho plazo, y tras obtener del Organismo de Certificación autorización escrita, procederá a su destrucción, de forma que se garantice que la información de las evaluaciones queda irreconocible y se impida su reconstrucción, total o parcial.

4. El Organismo de Certificación, previo a la autorización de destrucción, podrá requerir al laboratorio el traslado de cuanta información de las evaluaciones sea de su interés.

**Artículo 37.** *Inventario anual.*

El laboratorio presentará ante el Organismo de Certificación, antes del diez de enero de cada año, un inventario anual de toda la información de las evaluaciones que obran en su poder a fecha treinta y uno de diciembre del año anterior.

Subsección 3.ª Servicio de Protección de la información de las evaluaciones

**Artículo 38.** *Miembros del Servicio de Protección.*

1. En la organización del laboratorio, el Servicio de Protección de la información de las evaluaciones estará constituido, al menos, por el jefe del Servicio de Protección, el director del Servicio de Protección y el administrador de seguridad del sistema de información.

2. Los miembros del Servicio de Protección nombrados en el párrafo anterior son los responsables, ante el Organismo de Certificación, de la correcta aplicación de los requisitos de seguridad indicados, por ello deben contar con el adecuado grado de representatividad y autoridad, dentro de la organización del laboratorio.

3. Sus funciones de seguridad no podrán quedar disminuidas en ningún momento, aún cuando desempeñen otros cometidos en el laboratorio, debiendo contar con los medios necesarios para realizar sus funciones con eficacia.

**Artículo 39.** *Condiciones personales y nombramiento.*

1. Los responsables del Servicio de Protección deberán tener dependencia directa de la dirección del laboratorio, una relación laboral estable sobre la base de continuidad en su función y se les reconocerá, dentro del laboratorio, la debida autoridad en el desempeño de sus cometidos.

Deberán gozar de prestigio personal y profesional, y tener un amplio conocimiento de la organización del laboratorio.

2. El nombramiento y cese de los responsables del Servicio de Protección se comunicará por escrito, reconocido expresamente, en el que constarán las misiones de la responsabilidad asignada.

3. La inadecuación en el desarrollo, o la inobservancia, de las misiones encomendadas a los responsables del Servicio de Protección, podrá motivar su cese, cuando el Organismo de Certificación así lo demande, previa notificación por escrito, y sin perjuicio de la exigencia de otras responsabilidades que se pudieran derivar.

**Artículo 40.** *Director del Servicio de Protección.*

1. Cuando el laboratorio designe varios jefes del Servicio de Protección de la información de las evaluaciones, uno por cada una de las sedes donde se maneje o custodie información de las evaluaciones, deberá nombrar un director del Servicio de Protección, cuya misión principal será coordinar la actuación de dichos jefes, así como de los distintos administradores de seguridad del sistema de información, sin que esto suponga merma alguna de las responsabilidades que a éstos corresponde.

2. El cargo de director del Servicio de Protección se podrá compatibilizar con el de jefe de dicho Servicio, en las dependencias donde se ubiquen las oficinas centrales del laboratorio.

**Artículo 41.** *Misiones del jefe del Servicio de Protección.*

1. Corresponde al jefe del Servicio de Protección la misión de organizar, dirigir y controlar el sistema de protección para salvaguarda de la información de las evaluaciones, y la obligación de cumplir y hacer cumplir, en todas sus partes, estos requisitos de seguridad para la acreditación del laboratorio.

2. Entre los cometidos del jefe del Servicio de Protección se encuentran:

a) Asegurar la protección de la información de las evaluaciones en poder del laboratorio.

b) Regular el acceso a la información de las evaluaciones conforme a los criterios y procedimientos establecidos.

c) Llevar a cabo un programa de formación del personal del laboratorio, con una periodicidad mínima de treinta (30) meses, cuyo principal objetivo será sensibilizar a dicho personal sobre la importancia de cumplir los procedimientos de protección de la información de las evaluaciones y el deber de discreción.

d) Controlar la recepción, custodia, reproducción, destrucción y devolución de la información de las evaluaciones, conforme a los procedimientos establecidos.

e) Velar, especialmente, para que ninguna información de las evaluaciones sea transmitida indebidamente, o sea manejada o custodiada en lugar distinto a las zonas protegidas.

f) Elaborar, implantar y mantener el Plan de Protección conforme a lo establecido en este Reglamento.

g) Mantener actualizados los registros de seguridad.

**Artículo 42.** *Misión del administrador de seguridad del sistema de información.*

1. El administrador de seguridad del sistema de información tendrá como misión organizar, dirigir y controlar la seguridad del sistema de información del laboratorio. Este administrador podrá ser el propio jefe del Servicio de Protección, cuando tenga la formación adecuada.

2. Entre los cometidos del administrador de seguridad del sistema de información se encuentran:

a) Elaborar, organizar e implementar los requisitos y procedimientos relativos a la seguridad de los sistemas de información del laboratorio, debiendo revisar, periódicamente, la eficacia de todos los componentes.

b) Controlar que todo el personal que tiene acceso al sistema de información está debidamente autorizado.

c) Investigar los incidentes de seguridad que pudieran afectar al sistema de información, evaluando en su caso, los daños causados e informando de las conclusiones al jefe del Servicio de Protección.

d) Llevar a cabo un programa de formación continua de los usuarios del sistema de información, sobre la observancia de los procedimientos de seguridad.

e) Gestionar y proporcionar los códigos de acceso u otros dispositivos de control de acceso al sistema de información. Llevará un registro de asignación de códigos a los usuarios, que serán cambiados con una periodicidad mínima de tres meses, y cada vez que se produzca, o se sospeche que haya ocurrido, un incidente de seguridad que comprometa dichos códigos.

f) Realizar la gestión de claves del sistema de información del laboratorio, incluidos los sistemas de cifra que estuvieran en el ámbito de su competencia, así como la de los sistemas de soporte a la evaluación. Para ello, controlará su generación, almacenamiento, distribución, expiración y destrucción. En la recepción de nuevos equipos modificará todas las claves que, por defecto, vengan de fábrica.

g) Controlar tanto las modificaciones que se realicen en cualquier componente del sistema de información, asegurándose que no se vea afectada la seguridad del sistema, como los aspectos de la gestión de la configuración de dichas modificaciones.

h) Comprobar que el mantenimiento del sistema de información se realiza conforme a los procedimientos y requisitos operativos de seguridad.

i) Verificar que los soportes de almacenamiento que incluyan información de las evaluaciones se custodian debidamente.

j) Evaluar los registros de seguridad del sistema de información, asegurándose que son suficientes para llevar a cabo un control eficaz. Deberán incluir aquellas actividades, con indicación del usuario, hora y fecha, en que se produzcan hechos que puedan afectar a la seguridad del sistema, como finalizaciones anormales del trabajo, cierres indebidos del sistema, fallos en los mecanismos de seguridad, intentos no autorizados de acceso a datos de la evaluación, uso del sistema de un modo no autorizado, copias e impresiones de la información de las evaluaciones, etc.

k) Controlar y registrar las copias periódicas de seguridad.

Subsección 4.ª Inspecciones de seguridad

**Artículo 43.** *Inspectores de seguridad.*

Los inspectores de seguridad son los representantes del Organismo de Certificación, ante el laboratorio, para la comprobación de la correcta aplicación de los requisitos de seguridad exigidos en el proceso de acreditación.

El laboratorio les reconocerá las competencias que les atribuyen estos requisitos, asumiendo el compromiso de facilitarles su labor, y dispondrá los medios precisos para que realicen sus funciones con eficacia.

**Artículo 44.** *Nombramiento.*

El Organismo de Certificación notificará al laboratorio la identidad del inspector de seguridad correspondiente, así como los cambios que se produzcan.

El nombramiento de inspector de seguridad, para un mismo laboratorio, podrá recaer en varias personas, si el Organismo de Certificación así lo estima oportuno.

**Artículo 45.** *Misiones del inspector de seguridad.*

Corresponde al inspector de seguridad:

a) La observancia del exacto cumplimiento de las obligaciones y compromisos que contrae el laboratorio en el proceso de acreditación.

b) Asesorar al laboratorio en la puesta en práctica de los procedimientos de seguridad, que garanticen la protección de la información de las evaluaciones.

**Artículo 46.** *Inspecciones.*

1. La inspección constituye uno de los medios por los que el Organismo de Certificación comprueba el cumplimiento, por parte del laboratorio, de los requisitos de seguridad para la acreditación.

2. Las inspecciones serán ordinarias cuando se realizan de forma periódica, por los inspectores de seguridad nombrados específicamente para cada laboratorio. Las inspecciones ordinarias no precisan concertación previa.

3. Las inspecciones extraordinarias se realizarán cuando el Organismo de Certificación lo estime conveniente, y serán llevadas a cabo por las personas que éste designe. Las inspecciones extraordinarias se comunicarán previamente al laboratorio.

4. En las inspecciones estarán obligados a estar presentes, el jefe del Servicio de Protección, o quien le sustituya, debidamente acreditado en el caso justificado de que el primero no pudiera asistir, y el personal dependiente del laboratorio que designe el Organismo de Certificación.

5. El inspector de seguridad, en las inspecciones ordinarias, o el jefe de la comisión del Organismo de Certificación, en las inspecciones extraordinarias, deberá anotar en el registro del laboratorio, un resumen del resultado de la inspección. En el caso de presentar aspectos negativos, se remitirá al laboratorio la correspondiente comunicación, en la que se deberá reflejar el plazo de corrección para solventar las anomalías observadas por la inspección.

Subsección 5.ª Visitas

**Artículo 47.** *Consideración de visita.*

Se considera visita, el acceso físico y circunstancial de una o varias personas, sin relación de dependencia directa con el laboratorio, a las dependencias o instalaciones del mismo.

**Artículo 48.** *Registro de visitas.*

Las visitas se anotarán en el registro de visitas, antes de efectuar la visita. Se deberán recoger, como mínimo, los siguientes datos: fecha de la visita, nombre completo del visitante, número del DNI o pasaporte, nacionalidad, empresa/organismo o dirección del visitante, y nombre de la persona visitada.

Este registro estará a disposición del Organismo de Certificación, para su consulta.

**Artículo 49.** *Normas para el control de visitas.*

Para el control de las visitas, se seguirán las siguiente normas:

a) El laboratorio controlará el movimiento de las visitas que entren en sus dependencias, para garantizar la debida seguridad de la información de las evaluaciones que custodie.

b) Se prohibirá al visitante efectuar cualquier tipo de registro o reproducción de la información de las evaluaciones, que deberá solicitarse al personal del laboratorio y ser efectuado mediante los procedimientos correspondientes.

c) Toda entrega al visitante de información de las evaluaciones será anotada en el registro.

**Artículo 50.** *Visitas de larga duración.*

Tendrán consideración de visitas de larga duración, las realizadas sobre la base de continuidad o reiteración, por un periodo de doce meses. Tales visitas se anotarán en el registro de seguridad de personal, incluyendo las autorizaciones de acceso a la información de evaluaciones que se pudieran conceder.

Subsección 6.ª Zonas de acceso restringido

**Artículo 51.** *Sistema de protección.*

1. El laboratorio implantará un sistema de protección, integrado en la estructura empresarial, que permita proteger la información de las evaluaciones contra los riesgos que puedan implicar una amenaza para la misma.

2. El sistema de protección puede entenderse como el conjunto de recursos y procedimientos que, interactuando coordinadamente, tienen como finalidad proteger la información de las evaluaciones de los riesgos que puedan afectar a su integridad, confidencialidad o disponibilidad.

**Artículo 52.** *Características del sistema de protección.*

El documento donde se definen las características que presenta el sistema de protección es el Plan de Protección, definido en el Artículo 26.

El laboratorio deberá adjuntar, al Plan de Protección, un proyecto del subsistema de protección física, que estará compuesto por una memoria justificativa de los criterios de diseño, la descripción detallada de todos los componentes de la instalación y los planos que especifiquen la ubicación física de los mencionados componentes.

**Artículo 53.** *Subsistema de protección física.*

El subsistema de protección física, que ha de instalarse, obligatoriamente, en las dependencias del laboratorio donde se vaya a manejar información de las evaluaciones, ha de mantenerse en un óptimo grado de eficacia y utilidad para el cumplimiento de las condiciones de acreditación del laboratorio. La valoración de dicha eficacia y utilidad corresponde al Organismo de Certificación.

Las áreas de acceso restringido, que deberá considerar el subsistema de protección física, están compuestas por las zonas de evaluación y las zonas de protección.

**Artículo 54.** *Zonas de evaluación.*

Las zonas de evaluación son las constituidas por aquellas dependencias del laboratorio en las que, únicamente, se debe manejar y custodiar información de las evaluaciones, con las siguientes características:

a) Ha de estar construida de forma que quede limitado, materialmente, el acceso a la misma, y de manera que se pueda apreciar, con una simple inspección, una intrusión a través de las paredes, suelo, puertas o ventanas que delimiten la zona. Estos elementos no deben permitir la observación desde el exterior.

b) Las puertas de acceso deben disponer de una cerradura de bloque con llave, cuyo mecanismo será obligatoriamente accionado, cuando en el interior se esté trabajando con información de las evaluaciones, así como cuando no haya nadie en la misma. También dispondrán de un dispositivo que obligue a la puerta a permanecer cerrada, cuando no se esté franqueando, y dispondrán de detector de apertura.

c) Si se incluyen ventanas, deben colocarse dispositivos que detecten su apertura, en el caso de ser practicables, así como detectores de rotura de cristales. Los elementos translúcidos deberán estar acondicionados para impedir la observación desde el exterior. En el caso de que las ventanas tengan fácil acceso desde el exterior, estarán físicamente protegidas.

d) Se implantarán medidas físicas y organizativas para impedir el acceso a la zona de evaluación, al personal que no tenga derecho de acceso a la información de las evaluaciones y, en el caso en que se divida esta zona por evaluaciones, al personal que no tenga derecho de acceso, en particular, a la información de la evaluación asociada a cada división.

e) Deberá contar con una caja fuerte Nivel IV, conforme a la norma UNE-EN 1143-1-98, equipada con cerradura Clase B, según norma EN 1300, donde se custodiará, obligatoriamente, la información de las evaluaciones durante los períodos de tiempo en que no se esté manejando. Deberá reunir, además, las características siguientes:

Si se trata de caja fuerte autónoma, ha de estar anclada si su volumen es inferior a 500 litros, o si su peso no supera los 1.000 Kg.

Si se trata de caja fuerte empotrada, el grado de seguridad del alojamiento donde se ubique ésta ha de proporcionar, como mínimo, el atribuido al de la puerta y marco de la caja.

Doble sistema de apertura, uno de los cuales ha de ser, ineludiblemente, de combinación electrónica.

**Artículo 55.** *Zonas de protección.*

Las zonas de protección son las constituidas por el entorno de las zonas de evaluación en el que no se podrá manejar o custodiar información de las evaluaciones, pero que estarán dotadas de medidas de seguridad, con la finalidad de incrementar la seguridad de las zonas de evaluación y tendrán las siguientes características:

a) Su ubicación dependerá de las características constructivas y de la situación de la zona de evaluación.

b) En cualquier caso, se implementarán las medidas físicas y organizativas suficientes para que el personal que acceda a la zona de protección esté identificado.

**Artículo 56.** *Central de alarmas.*

Además de los requisitos establecidos en los artículos 54 y 55, las zonas de evaluación y de protección dispondrán de las siguientes medidas de seguridad:

a) Todos los medios activos de seguridad deben estar conectados físicamente a un centro de control de alarmas, que disponga de una autonomía mínima de setenta y dos horas, provista de un dispositivo antisabotaje y ubicada de manera oculta.

b) Este centro de control quedará activado, obligatoriamente, fuera del horario laboral y estará conectado con una central receptora de alarmas, que pueda gestionar cualquier alarma de forma oportuna.

c) La conexión con la central receptora de alarmas debe permitir la verificación automática de la línea de comunicación, para poder conocer oportunamente una interrupción en la misma, a través de la correspondiente señal de alarma. La operativa de la gestión de la central receptora de alarmas deberá estar incluida en el Plan de Protección.

d) Los códigos de acceso de la central de alarmas, que permiten su programación y control, deberán ser conocidos, únicamente, por el jefe del Servicio de Protección y las personas por él designadas. Dicha designación quedará anotada en el registro de seguridad del personal. Los códigos deberán modificarse con los criterios indicados en el artículo 57, referido a «Combinaciones, códigos de acceso y control de llaves», que sigue.

Subsección 7.ª Procedimiento de seguridad

**Artículo 57.** *Combinaciones, códigos de acceso y control de llaves.*

1. Sólo tendrán conocimiento de los códigos de acceso a las zonas de evaluación, de las claves de control de la central de alarmas, así como de las combinaciones de los lugares de

custodia de la información de las evaluaciones, el jefe del Servicio de Protección y las personas que él designe, que serán las mínimas imprescindibles.

2. Las llaves de las cajas fuertes no podrán salir de la sede del laboratorio bajo ningún concepto, debiendo guardarse de forma oculta y segura, y en distinto lugar al que se custodien las claves de combinación para la apertura de las mismas.

3. Deberá ocultarse la identificación del fabricante, modelo, año de construcción u otros datos que puedan facilitar un conocimiento de las características de las cajas fuertes a las que se refieren.

4. Las claves de combinación para la apertura de las cajas fuertes y los códigos de control de la central de alarmas no deben conservarse en claro, sino de manera cifrada, debiendo ser modificados, obligatoriamente, en los siguientes casos:

a) Al recibirse los muebles de seguridad e instalarse la central de alarmas, modificando las claves y códigos que traen de fábrica.

b) Cada seis meses.

c) Cuando se produzca un cambio en las personas que hayan tenido acceso a las mismas, incluido el personal de las empresas de mantenimiento.

d) Cada vez que se produzca, o se sospeche que haya ocurrido, un incidente de seguridad que comprometa las claves o los códigos.

**Artículo 58.** *Acceso físico a la información de las evaluaciones.*

Cuando se precise el acceso físico a la información de las evaluaciones, el jefe del Servicio de Protección de la información, o persona designada por él, pondrá dicha información a disposición de los empleados del laboratorio que cuenten con las debidas autorizaciones de acceso a la misma, la cual deberá ser manejada exclusivamente en la zona de evaluación, estando bajo la responsabilidad de estas personas su custodia y control.

Una vez finalizado el manejo, se devolverá inmediatamente a la persona que hizo entrega de la misma, siendo almacenada en su lugar de custodia, donde permanecerá obligatoriamente.

**Artículo 59.** *Dispositivos técnicos de identificación.*

Siempre que el laboratorio lo considere necesario, podrá emplear dispositivos personales que faciliten y controlen el acceso, por su personal, a las zonas de acceso restringido. Los dispositivos serán diseñados de forma que se impida su empleo no autorizado, por lo que, cada uno de ellos se asignará a un empleado determinado, con su correspondiente código personalizado, que será conocido únicamente por el interesado.

De estos dispositivos no podrán determinarse las evaluaciones a cuya información tiene acceso el empleado al que se le asigna.

En su caso, deberá notificarse al Organismo de Certificación el sistema adoptado, debiéndose plasmar la operativa del mismo en el Plan de Protección.

Subsección 8.ª Seguridad de los sistemas de información

**Artículo 60.** *Seguridad de la información sobre evaluaciones.*

1. La información de las evaluaciones es un bien que debe ser protegido de manera que se garantice su confidencialidad, su integridad y disponibilidad, a lo largo de toda su existencia, con independencia del medio, soporte o formato en el que permanezca o se transmita. Para ello, también es necesario asegurar la integridad y disponibilidad de los servicios y recursos que sustentan dicha información.

2. Los mecanismos de seguridad del sistema de información que procese, almacene o transmita información de las evaluaciones, tienen como finalidad evitar accesos, destrucciones y modificaciones no permitidas, asegurando, al mismo tiempo, que la información es utilizada cuándo y cómo lo requieran los usuarios autorizados.

3. Los factores que se han de evaluar en la protección de la información de las evaluaciones serán los siguientes:

a) Confidencialidad, como servicio de seguridad que pretende que una información sea revelada exclusivamente a los usuarios, entidades o procesos autorizados.

b) Integridad, como medida que asegura que la información sea creada, modificada o borrada sólo por personas, entidades o procesos autorizados.

c) Disponibilidad, para que la información sea utilizable en el lugar, momento y forma que lo requieran lo usuarios, entidades o procesos autorizados.

4. El laboratorio deberá concretar los principios y reglas básicas de seguridad, exigidos para la acreditación, en unos procedimientos específicos para la protección de la información de las evaluaciones tratadas en su sistema de información, cuya seguridad deberá estar necesariamente integrada en el sistema de protección del laboratorio.

5. La seguridad del sistema de información requiere la adecuada aplicación de procedimientos y normas que posibiliten el control de acceso al sistema, la distribución de responsabilidades, la segregación de funciones y la compartimentación de los entornos correspondientes a las evaluaciones y a la administración y gestión del laboratorio.

**Artículo 61.** *Usuario del sistema de información.*

1. El usuario del sistema de información que maneje información de las evaluaciones dependerá directamente, en todo lo referente a la seguridad del sistema, del administrador de seguridad del sistema de información, al que informará inmediatamente del menor indicio o conocimiento de cualquier hecho que afecte a la seguridad de la información de las evaluaciones.

2. La responsabilidad de cada usuario es básica para la seguridad del sistema. Por ello es imprescindible la autenticación del usuario. Se entenderá por autenticación el proceso que confirma su identidad.

Bajo ningún concepto este usuario podrá emplear equipos y medios particulares para el tratamiento de la información de las evaluaciones.

El usuario se asegurará que su código personal no es utilizado por otra persona, recomendándose la memorización del mismo, sin dejar constancia escrita o, en su caso, guardando el registro de forma oculta y segura; no hacer uso del código cuando se está siendo observado y no compartir, en ningún caso, el código personal con otros usuarios del sistema.

3. En los sistemas que lo permitan, el usuario realizará copias periódicas de seguridad de la información de las evaluaciones, bajo la supervisión del administrador de seguridad del sistema de información, quien llevará el control y registro oportuno.

**Artículo 62.** *Soportes de almacenamiento de información de las evaluaciones.*

1. Los soportes removibles reutilizables, que hayan contenido información de las evaluaciones, podrán volverse a emplear una vez que se haya efectuado el borrado seguro mediante procedimientos que garanticen el mismo.

Esto también se aplicará a los soportes fijos de los equipos utilizados en las pruebas de evaluación, así como en los destinados a la instalación, o recreación, del producto a evaluar y a su entorno de pruebas, que deberán borrarse de manera segura al término de cada evaluación.

El resto de soportes fijos de información del laboratorio deberán ser tratados según procedimientos específicos, que serán reseñados en los Procedimientos Operativos de seguridad, de forma que se imposibilite la extracción de información por personal no autorizado.

2. Toda información que tenga entrada mediante comunicaciones electrónicas, o soporte removible, deberá ser comprobada en un sistema aislado, previamente a su inclusión en el sistema de información del laboratorio, a fin de detectar la posible presencia de elementos extraños, dañinos o de mal funcionamiento. Dicha comprobación, y su resultado, quedarán anotados en el libro registro del laboratorio junto con la anotación de la entrada de la información.

**Artículo 63.** *Características físicas de las instalaciones.*

1. El sistema de información que se utilice para el tratamiento de la información de las evaluaciones deberá estar situado en la zona de evaluación y, obligatoriamente, ubicado en territorio nacional.

2. Los equipos periféricos de impresión de documentos estarán insonorizados, cuando las características de los mismos lo requieran, y así lo determine el Organismo de Certificación.

3. No se podrá realizar ningún cambio en la ubicación física de los elementos del sistema de información, sin el control del administrador de seguridad, y la aprobación del jefe del Servicio de Protección de la información de las evaluaciones.

**Artículo 64.** *Procedimientos operativos de seguridad.*

1. El administrador de seguridad del sistema de información del laboratorio elaborará unos Procedimientos Operativos de seguridad, donde se describirán, detalladamente, las operaciones necesarias para proteger dicho sistema.

2. Estos procedimientos operativos de seguridad han de cumplir los requisitos de seguridad para la acreditación del laboratorio, incluirse en el Plan de Protección y, adicionalmente, contemplarán lo siguiente:

a) La revisión bianual del grado de cumplimiento de la eficacia de los propios procedimientos operativos, y del cumplimiento de los requisitos de seguridad para la acreditación del laboratorio.

b) La aplicación de medidas de protección contra elementos dañinos o maliciosos (virus, caballos de Troya, gusanos, etc.).

c) El cambio trimestral de los códigos de acceso de los usuarios.

d) La aplicación de un sistema de borrado rápido o destrucción de la información de las evaluaciones, para casos de emergencia.

e) La utilización de un sistema de alimentación ininterrumpida, de duración suficiente, para salvaguardar los procesos en curso.

**Artículo 65.** *Interconexión de sistemas.*

1. Como norma general, el sistema de información donde se trate información de las evaluaciones, deberá estar aislado.

Excepcionalmente pueden existir situaciones en las que el sistema necesite estar interconectado con otros, bien para comunicar varias zonas de evaluación del laboratorio, separadas físicamente, en las que se realice la misma evaluación, o para permitir la comunicación en situaciones de naturaleza análoga.

En estas situaciones, la interconexión deberá ser autorizada por el Organismo de Certificación, que determinará los requisitos de seguridad que se deben implantar.

2. El acceso del laboratorio a redes públicas, para la consulta y descarga de información de vulnerabilidades, programas de uso en las evaluaciones y demás información relevante a las evaluaciones, no se podrá realizar en las áreas de evaluación o de protección, debiendo tramitarse la incorporación de esta información al sistema de información del laboratorio, conforme a lo requerido en el artículo 32, «Libro registro de información de las evaluaciones».

### *Sección 3.ª Requisitos de los procedimientos de evaluación*

**Artículo 66.** *Reconocimiento de actuaciones del laboratorio de evaluación.*

La certificación de la seguridad de un producto se inicia a instancias del solicitante ante el Organismo de Certificación, lo cual no obsta para que, independientemente, se puedan solicitar, por parte del mismo interesado, trabajos de evaluación equivalentes a los que requiere el Organismo de Certificación para la certificación de dicho producto.

En cualquier caso, el Organismo de Certificación únicamente reconocerá las actuaciones del laboratorio de evaluación que se realicen, completamente, bajo su conocimiento y

seguimiento, conforme al procedimiento establecido en el Capítulo V del presente Reglamento.

**Artículo 67.** *Procedimientos de evaluación.*

Los procedimientos de evaluación del laboratorio que solicite la acreditación, deberán contemplar las obligaciones de coordinación e información con el Organismo de Certificación, indicadas en esta Sección.

Igualmente, y para la defensa de la validez y reconocimiento mutuo de certificados de la seguridad de los productos, el Organismo de Certificación trasladará al laboratorio las obligaciones requeridas, tanto al procedimiento de evaluación, como a los propios laboratorios de evaluación, en los acuerdos, convenios o contratos de reconocimiento mutuo en los que el solicitante de la certificación del producto quiera hacer valer la misma y el Organismo de Certificación opere.

**Artículo 68.** *Obligaciones de coordinación e información.*

El laboratorio deberá cumplir, en el desarrollo de sus trabajos de evaluación, con los requisitos de coordinación e información con el Organismo de Certificación que se incluyen en esta Sección.

**Artículo 69.** *Aprobación previa.*

1. El laboratorio de evaluación estará obligado a obtener aprobación previa, y por escrito, del Organismo de Certificación para comenzar los trabajos de evaluación.

En la aprobación previa deberá constar la asignación del responsable de la certificación del producto, por parte del Organismo de Certificación, a quien se dirigirán las comunicaciones relativas a la evaluación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

2. Dicha aprobación se solicitará por el laboratorio mediante escrito, al que se acompañará lo siguiente:

a) Plan detallado de la evaluación, con las fases, tareas y unidades de trabajo correspondientes, la asignación e identificación del personal afecto a la evaluación y su responsabilidad en la misma.

b) Copia del contrato, o documento similar, que regule las relaciones entre el laboratorio y el solicitante de la certificación, en las que el laboratorio incluirá, obligatoriamente, las cláusulas necesarias para el cumplimiento de los requisitos para la acreditación del laboratorio.

**Artículo 70.** *Inicio y fin de los trabajos de evaluación.*

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, el comienzo y término de cada fase, actividad, acción y unidad de trabajo de la evaluación, según se definan en la metodología y procedimientos de evaluación a aplicar. En función de su relevancia, el Organismo de Certificación podrá rebajar este requisito a la comunicación de fases, actividades o hitos señalados.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

**Artículo 71.** *Desviaciones del plan de evaluación.*

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, las desviaciones con respecto al plan de evaluación, con análisis de las causas de la desviación, las medidas correctivas aplicadas por el laboratorio, y el nuevo plan de evaluación actualizado.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

**Artículo 72.** *Dificultades en la evaluación.*

El laboratorio de evaluación estará obligado a comunicar, al Organismo de Certificación, cualquier dificultad surgida en la aplicación o interpretación de las normas utilizadas, así como cualquier dificultad que condicione el normal transcurso de una evaluación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

**Artículo 73.** *Informes de observación.*

El laboratorio estará obligado a remitir, al Organismo de Certificación, todos los informes de observación y de disconformidad emitidos e informará de su cierre, cuando ocurra, y de las medidas correctivas aplicadas por el solicitante de la certificación.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

**Artículo 74.** *Información técnica adicional.*

El laboratorio de evaluación estará obligado a facilitar toda información técnica adicional que sea necesaria para el análisis, por parte del Organismo de Certificación, de la información de las evaluaciones, incluyendo acceso y formación sobre programas y sistemas de evaluación, elaborados o adquiridos por el laboratorio, así como aquellos métodos y técnicas de análisis de vulnerabilidades empleados.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

**Artículo 75.** *Reuniones entre el solicitante y el laboratorio.*

El laboratorio de evaluación estará obligado a comunicar, e invitar a su asistencia, al Organismo de Certificación, de cuantas reuniones celebre dicho laboratorio con el solicitante de la certificación, con indicación de su naturaleza y objeto.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

**Artículo 76.** *Reuniones de seguimiento.*

El laboratorio de evaluación estará obligado a atender cuantas reuniones de seguimiento convoque el Organismo de Certificación. Dichas reuniones se convocarán por el responsable de la certificación del producto del Organismo de Certificación, y serán atendidas por el personal requerido para explicar e interpretar la información de las evaluaciones objeto de seguimiento. En el caso de información de las evaluaciones elaborada por el laboratorio, se podrá requerir la asistencia a la reunión de los autores de la misma.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

**Artículo 77.** *Puesta a disposición de dependencias y sistemas.*

El laboratorio de evaluación estará obligado a poner sus dependencias y sistemas de evaluación a disposición del Organismo de Certificación, para la realización, por parte del personal del mismo, de las tareas de verificación de la actividad de evaluación que se consideren oportunas.

Esta obligación deberá estar recogida en los procedimientos de evaluación propios del laboratorio.

CAPÍTULO IV

## Acreditación de laboratorios

### *Sección 1.ª Acreditación*

**Artículo 78.** *Acreditación.*

El Organismo de Certificación acreditará a los laboratorios solicitantes siguiendo el procedimiento establecido en la Sección 4.ª de este Capítulo y en base al cumplimiento de los requisitos establecidos en el Capítulo III.

**Artículo 79.** *Solicitantes.*

Pueden solicitar esta acreditación cualesquiera laboratorios de evaluación de la seguridad de los sistemas de información, con independencia de su naturaleza jurídica, pública o privada, sin más limitación que la de realizar su actividad de evaluación en territorio español.

**Artículo 80.** *Contenido de la acreditación.*

La acreditación de un laboratorio supone el reconocimiento de su competencia técnica, de la adecuación de la gestión de la seguridad del mismo a las particularidades de la evaluación de la seguridad de las Tecnologías de la Información, y de la consideración de los requisitos de coordinación e información al Organismo de Certificación, que permitirá a éste basar su dictamen de certificación de un producto, entre otros factores, en el informe de evaluación del laboratorio acreditado.

La acreditación de un laboratorio no presupone, sin embargo, aceptación incondicional de los resultados de la actuación de evaluación de un producto determinado. Dicha aceptación se otorgará tras el análisis inicial de la solicitud de certificación, mediante el seguimiento de la labor de evaluación y tras el análisis del correspondiente informe técnico de evaluación, tal y como se define en el Capítulo V.

**Artículo 81.** *Duración de la acreditación.*

La acreditación, una vez concedida, se mantiene de manera indefinida, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del laboratorio. Para el mantenimiento de la acreditación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del laboratorio y de su actuación, conforme se regula en este Capítulo.

### *Sección 2.ª Alcance de la acreditación*

**Artículo 82.** *Alcance de la acreditación.*

La acreditación se cualifica mediante el alcance, que limitará el reconocimiento de las actuaciones del laboratorio con relación al nivel de calificación de seguridad y con relación a las normas y niveles de evaluación.

**Artículo 83.** *Alcance con relación al nivel de calificación de seguridad.*

Con relación al nivel de calificación de seguridad se distinguen aquellos laboratorios con capacidad para manejar información y productos clasificados, de aquellos otros que operan en el régimen de la información y productos no clasificados.

**Artículo 84.** *Alcance con relación a las normas y niveles de evaluación.*

La certificación de la seguridad de los productos y sistemas de las Tecnologías de la Información puede requerir la evaluación de los mismos atendiendo a diferentes criterios, métodos y normas de evaluación.

Adicionalmente, dichas normas pueden distinguir niveles de evaluación y niveles de seguridad.

El Organismo de Certificación mantiene una relación actualizada de normas aplicables, según se establece en el Capítulo VI.

El laboratorio solicitante deberá indicar, en el alcance de la acreditación, aquellas normas y niveles, de la mencionada relación, en las que demuestra competencia técnica y experiencia acreditada.

### *Sección 3.ª Criterios de acreditación*

**Artículo 85.** *Criterios generales.*

1. La competencia técnica del laboratorio solicitante se determinará, en primera instancia, por la correspondiente acreditación de esta competencia, conforme a lo regulado en la Ley 21/1992, de 16 de julio, de Industria, y en el Real Decreto 2200/1995, de 28 de diciembre, por el que se aprueba el Reglamento de la Infraestructura para la Calidad y Seguridad Industrial, y en base al cumplimiento, por parte del laboratorio, de la norma UNE-EN ISO/IEC 17025.

2. La acreditación de competencia técnica, que deberá ser concedida por una entidad de acreditación reconocida, ha de incluir, en su alcance, las normas de evaluación de la seguridad de los productos y sistemas de Tecnologías de la Información, aprobados por el Organismo de Certificación, y demás limitaciones requeridas por éste.

En particular, se reconocen las acreditaciones de competencia técnica emitidas por la Entidad Nacional de Acreditación, sin perjuicio de las acreditaciones emitidas por otras entidades de acreditación que satisfagan los requisitos establecidos en el Capítulo II del Reglamento de la Infraestructura para la Calidad y Seguridad Industrial.

3. Los requisitos adicionales, de gestión de la seguridad de la información de las evaluaciones, así como los de coordinación e información al Organismo de Certificación, se incluyen en el Capítulo III.

Los requisitos indicados en el párrafo anterior, se verificarán mediante la aplicación del procedimiento establecido en la siguiente Sección, sobre la base de una auditoría del laboratorio solicitante, que incluye el seguimiento de una evaluación de prueba bajo los procedimientos y requisitos del Organismo de Certificación.

**Artículo 86.** *Criterios complementarios.*

Para aquellos casos que lo requieran, los criterios generales mencionados podrán ser completados o precisados por otros complementarios de carácter técnico, específicos para cada tipo de producto a evaluar, criterios, métodos y normas de evaluación de cada acreditación, o modificación del alcance de la solicitada, recogidos y publicados en los correspondientes documentos del Organismo de Certificación.

### *Sección 4.ª Procedimiento de acreditación*

**Artículo 87.** *Proceso de acreditación.*

Aquellos laboratorios que deseen ser acreditados por el Organismo de Certificación, deberán someterse al proceso de acreditación establecido en la presente Sección.

**Artículo 88.** *Solicitud de acreditación.*

La solicitud de acreditación deberá remitirse al Director del Organismo de Certificación adjuntando, como mínimo, la siguiente información, debidamente documentada:

a) Personalidad jurídica de la entidad solicitante, con su número de identificación fiscal.

b) Nombre del responsable del laboratorio y de la persona, o personas, con capacidad suficiente para obrar, que serán signatarias y, por tanto, responsables de la veracidad de las evaluaciones para las que el laboratorio solicita ser acreditado.

c) Compromiso de cumplir los requisitos de acreditación del Organismo de Certificación, indicados en el Capítulo III, así como declaración de disponibilidad para la realización de la auditoría y actividades derivadas del proceso de acreditación.

d) Relación y ubicación de las dependencias, delegaciones e instalaciones donde se realiza la actividad de evaluación de la seguridad de los productos y sistemas de las Tecnologías de la Información.

e) Alcance de la acreditación solicitada, indicando el nivel de calificación de seguridad y las normas y niveles de evaluación.

f) Relación y copia de los documentos del sistema de gestión de la calidad del laboratorio.

g) Relación y copia de los documentos del sistema de gestión de la seguridad del laboratorio.

h) Relación y copia de los manuales y procedimientos de evaluación del laboratorio.

i) Certificado de acreditación de la competencia técnica emitido por ENAC, o entidad de acreditación reconocida, según lo indicado en el artículo 85 o, en su caso, certificado de haber iniciado dicho proceso de acreditación con la entidad correspondiente.

j) Justificante del pago de las tasas de acreditación vigentes.

k) Alcance y descripción de las evaluaciones de prueba que el solicitante pretende llevar a cabo, bajo las condiciones y procedimientos de este esquema, para la demostración del cumplimiento de los requisitos de acreditación, y que han de ser de alcance igual, o superior, al de la acreditación solicitada.

Esta solicitud podrá presentarse en cualquiera de los lugares previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

**Artículo 89.** *Modelo de solicitud de acreditación.*

Las solicitudes de acreditación de laboratorio se presentarán en los impresos establecidos al efecto, que estarán publicados en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es).

**Artículo 90.** *Subsanación y mejora de la solicitud de acreditación.*

A la recepción de la solicitud de acreditación, el Organismo de Certificación realizará una comprobación inicial de la información en ella contenida.

En caso de ser necesaria la subsanación o mejora de la solicitud de acreditación, se estará a lo dispuesto en el artículo 71 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Se admitirá durante la instrucción de la solicitud de acreditación la equivalencia del certificado de acreditación de la competencia técnica por certificado de encontrarse incurso en el proceso de acreditación de dicha competencia, siendo requisito definitivo para la acreditación del laboratorio, la certificación de su competencia técnica conforme a lo indicado en el artículo 85.

**Artículo 91.** *Notificación al solicitante.*

El Organismo de Certificación notificará al solicitante el inicio del procedimiento administrativo de acreditación, incluyendo en dicha notificación:

a) El nombre y datos de contacto del responsable del procedimiento de acreditación, que será igualmente responsable de la dirección de la auditoría inicial del cumplimiento de los requisitos para la acreditación.

b) La fecha propuesta de comienzo de la auditoría indicada.

**Artículo 92.** *Preparación de la auditoría.*

Los técnicos designados por el Organismo de Certificación, con carácter previo a la auditoría, realizarán un estudio preliminar de la documentación recibida junto con la solicitud, relativa a los sistemas de calidad, seguridad y evaluación del laboratorio solicitante.

Las conclusiones de dicho estudio, en términos de observaciones sobre el cumplimiento e identificación de disconformidades de los requisitos para la acreditación, se remitirán al solicitante con una antelación no inferior a un mes de la fecha de comienzo de la auditoría. Junto a dichas conclusiones, y a la vista del estudio realizado, el Organismo de Certificación

indicará la duración estimada de la auditoría, cuyo calendario definitivo se acordará en la fecha de comienzo de la misma.

El laboratorio solicitante podrá subsanar y mejorar la solicitud de acreditación en base a las conclusiones del estudio preliminar, con carácter previo a la realización de la auditoría.

**Artículo 93.** *Instrucción de la auditoría.*

La instrucción de la auditoría se realizará en tres fases: reunión inicial, desarrollo de la auditoría y reunión final.

a) Reunión inicial. En la fecha indicada por el Organismo de Certificación, se celebrará la reunión inicial de auditoría entre los representantes del laboratorio solicitante y el equipo auditor, designado por el Organismo de Certificación. En esta reunión se harán las presentaciones oportunas, se confirmará el plan y calendario de la auditoría y se revisarán las conclusiones del estudio preliminar de la solicitud.

b) Desarrollo de la auditoría. Durante esta fase se procederá a la observación del laboratorio solicitante durante la evaluación de prueba, y a la investigación del cumplimiento de los requisitos para la acreditación.

c) Reunión final. El equipo auditor se reunirá con los representantes de la entidad solicitante, con objeto de presentar un informe verbal de los resultados del desarrollo de la auditoría.

**Artículo 94.** *Informe del equipo auditor.*

El equipo auditor, en un plazo no superior a diez días contados desde la fecha de la reunión final de la auditoría, elaborará un informe con los resultados y con la información recopilada durante el desarrollo de la misma. Este informe será remitido al laboratorio solicitante para su conocimiento.

**Artículo 95.** *Audiencia previa.*

1. Una vez instruido el procedimiento de auditoría, se le pondrá de manifiesto al laboratorio solicitante y se le convocará a una reunión de audiencia previa a la resolución.

2. En dicha reunión, el Organismo de Certificación indicará la naturaleza, gravedad y consecuencias de las observaciones y disconformidades identificadas durante el procedimiento de auditoría, si las hubiere, con las implicaciones de las mismas en la resolución de la solicitud de acreditación.

3. El laboratorio solicitante, en un plazo no inferior a diez días ni superior a quince, podrá alegar y presentar los documentos y alegaciones que estime pertinentes.

4. Si antes del vencimiento del plazo, el laboratorio manifiesta su decisión de no efectuar alegaciones ni aportar nuevos documentos o justificaciones, se tendrá por realizado el trámite.

**Artículo 96.** *Resolución de la solicitud de acreditación.*

1. La resolución de la solicitud de acreditación se dictará de acuerdo con lo indicado en este artículo y en los plazos establecidos en el artículo 107, «Plazos y actos presuntos».

2. Esta resolución, de acuerdo con lo previsto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrá ser objeto de recurso potestativo de reposición ante el Director del Organismo de Certificación, cuya resolución pone fin a la vía administrativa, o ser impugnada directamente ante el orden jurisdiccional contencioso-administrativo.

3. La resolución de desestimación será motivada. La resolución de acreditación contendrá adicionalmente los siguientes extremos:

a) Alcance de la acreditación concedida.

b) La fecha en vigor de la acreditación y referencia a su vigencia.

**Artículo 97.** *Vigencia de la acreditación.*

1. La acreditación se concederá por plazo indefinido, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del laboratorio.

2. Para el mantenimiento de la acreditación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del laboratorio y de su actuación, conforme a lo establecido en el presente Reglamento.

**Artículo 98.** *Certificación del producto evaluado en el proceso de auditoría.*

Las evaluaciones utilizadas como prueba, en el proceso de auditoría del laboratorio, podrán servir de base para la correspondiente certificación de la seguridad de los productos evaluados, conforme a lo indicado en el Capítulo V.

### *Sección 5.ª Seguimiento de la actividad de evaluación*

**Artículo 99.** *Seguimiento continuo de la actividad de evaluación.*

El Organismo de Certificación, conforme al procedimiento de certificación de productos, establecido en el Capítulo V, realizará un seguimiento continuo de la actividad del laboratorio, a los efectos de la resolución de las solicitudes de certificación de productos.

Todas aquellas observaciones y disconformidades sobre los requisitos de acreditación del laboratorio, detectadas durante el seguimiento de las evaluaciones, serán comunicadas al laboratorio para su subsanación.

En el caso de disconformidad, o de no atender las observaciones realizadas, se estará a lo dispuesto en los artículos 104, 105 y 106.

**Artículo 100.** *Auditorías de seguimiento.*

1. De forma periódica, se realizarán auditorías de seguimiento a los laboratorios acreditados.

2. Los objetivos de las auditorías de seguimiento serán los siguientes:

a) Comprobar que la entidad ha respetado, durante el periodo transcurrido desde la última auditoría, los criterios establecidos para la concesión de la acreditación.

b) Verificar el cierre de las desviaciones detectadas en auditorías previas.

c) Examinar cualquier cambio en la organización, procedimientos y recursos de la entidad, para la realización de las actividades incluidas en el alcance de su acreditación.

d) Comprobar que se han respetado las obligaciones resultantes de la acreditación.

e) Comprobar la actividad de la entidad para el alcance acreditado.

3. La frecuencia de las auditorías se establecerá en función de los resultados de visitas previas.

4. La primera auditoría de seguimiento se programará en un plazo no superior a doce meses desde la fecha inicial de acreditación. Las siguientes auditorías de seguimiento se realizarán antes de transcurridos dieciocho meses desde la realización de la última visita.

5. Las auditorías de seguimiento se realizarán con el mismo grado de detalle y rigor que la auditoría inicial de acreditación.

6. En la instrucción y resolución de la auditoría de seguimiento se seguirá lo dispuesto en los artículos 93 y 94 y, en todo caso, se atendrá al procedimiento general administrativo.

**Artículo 101.** *Ampliación del alcance de una acreditación.*

Cuando un laboratorio, ya acreditado, desee ampliar el alcance de su acreditación deberá solicitar formalmente dicha ampliación. Para ello, deberá utilizar el formulario de solicitud correspondiente. Se aplicará el procedimiento indicado en el artículo 78 adaptado, según proceda, en función del volumen y carácter de dicha ampliación.

**Artículo 102.** *Notificación de cambios.*

1. El laboratorio deberá comunicar, al Organismo de Certificación, cualquier cambio que se proponga efectuar sobre las condiciones iniciales en que se concedió la acreditación y, en particular, los que afecten a lo siguiente:

a) Situación jurídica, comercial u organizativa del laboratorio.
b) Organización y gestión, cuando afecten a personal directivo o a puestos clave en la organización del laboratorio o de la empresa.
c) Políticas y procedimientos, cuando proceda.
d) Locales de ubicación del laboratorio.
e) Personal y otros recursos, cuando sean relevantes.
f) Documentos normativos incluidos en el alcance de la acreditación.

2. Ante una comunicación de cambio, el Organismo de Certificación procederá a su revisión y establecerá las actividades necesarias para el mantenimiento de la acreditación del laboratorio. Dichas actividades podrán consistir en acciones de auditoría, por parte del Organismo de Certificación, para comprobar el grado de cumplimiento de los requisitos de acreditación tras los cambios efectuados, así como en la actualización, por parte del laboratorio, de la documentación presentada en el proceso de acreditación.

**Artículo 103.** *Publicidad de las acreditaciones.*

El Organismo de Certificación podrá hacer pública la relación de laboratorios en proceso de acreditación, así como la de laboratorios acreditados incluyendo, en esta relación, la información del alcance de cada acreditación.

### *Sección 6.ª Formulación de observaciones, plazos y recursos*

**Artículo 104.** *Formulación de observaciones y retirada de la acreditación.*

El incumplimiento de las obligaciones derivadas de la acreditación, por parte de la entidad titular de la misma, dará lugar a la adopción de medidas, por parte del Organismo de Certificación, contra la entidad incumplidora.

Las medidas irán en función de la gravedad del incumplimiento y podrán consistir en formulación de observaciones, retirada parcial o retirada total de la acreditación.

**Artículo 105.** *Actuaciones irregulares e incumplimientos.*

Se entenderá por actuaciones irregulares e incumplimientos leves, aquellas actuaciones que, sin adecuarse a lo establecido en el presente Reglamento, no afecten a la validez final de la actividad de evaluación de la entidad ni a la seguridad de terceros.

Las actuaciones irregulares y los incumplimientos leves serán objeto de observación, que podrá notificarse por los equipos de auditoría y seguimiento de las evaluaciones. El laboratorio deberá subsanar la causa que dio lugar a las observaciones, en el plazo de diez días.

**Artículo 106.** *Retirada de la acreditación.*

El incumplimiento reiterado de los requisitos de acreditación, o la no subsanación reiterada de las observaciones recibidas, darán lugar a la retirada, total o parcial, de la acreditación a la que se refiera.

La resolución de retirada de acreditación se dictará, de oficio, por el Organismo de Certificación.

La retirada de la acreditación obligará al solicitante al cese inmediato del uso de la condición de laboratorio acreditado, así como a la retirada de esta condición en todos los documentos o información en los que éste la haga manifiesta.

**Artículo 107.** *Plazos y actos presuntos.*

El plazo para resolver la solicitud de acreditación de laboratorio, y notificar la correspondiente resolución, será de seis meses. Este mismo plazo se aplicará a las solicitudes de ampliación del alcance de una acreditación previa.

A los efectos previstos en el artículo 43 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, las solicitudes de acreditación se entenderán estimadas de no recaer resolución expresa en los plazos establecidos en cada caso, con las salvedades y excepciones indicadas en dicho precepto.

**Artículo 108.** *Recursos.*

La actuación del Organismo de Certificación debe siempre atenerse a los principios generales de actuación recogidos en el artículo 3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

De acuerdo con lo previsto en los artículos 116 y 117 de la citada Ley, así como en los artículos 10, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, frente a la actuación del Organismo de Certificación, en materia de acreditación, se podrá interponer:

a) En el plazo de un mes, recurso potestativo de reposición ante el Director de dicho organismo, cuya resolución pone fin a la vía administrativa, o

b) Directamente, en el plazo de dos meses, recurso contencioso-administrativo, ante la Sala de dicha índole, del Tribunal Superior de Justicia de Madrid.

## CAPÍTULO V

## Certificación de productos y sistemas

### *Sección 1.ª Certificación*

**Artículo 109.** *Certificación de seguridad de productos y sistemas.*

El Organismo de Certificación certificará la seguridad de los productos y sistemas de Tecnologías de la Información, siguiendo el procedimiento establecido en este Capítulo y tras considerar, entre otras pruebas de la instrucción del procedimiento, los informes de evaluación emitidos por los laboratorios acreditados conforme a lo establecido en el Capítulo IV, y realizados atendiendo a los criterios, métodos y normas de evaluación de la seguridad indicados en el Capítulo VI.

**Artículo 110.** *Reconocimiento de veracidad de propiedades de seguridad.*

La certificación de la seguridad de un producto o sistema de las Tecnologías de la Información supone el reconocimiento de la veracidad de las propiedades de seguridad de su correspondiente declaración de seguridad.

**Artículo 111.** *Valoración de idoneidad.*

La certificación de la seguridad de un producto o sistema no presupone declaración de idoneidad de uso en cualquier escenario o ámbito de aplicación. Para valorar la idoneidad de un producto o sistema deberán tenerse en cuenta otras circunstancias, incluidas las restricciones establecidas en su declaración de seguridad para la correcta interpretación del certificado.

**Artículo 112.** *Vigencia de la certificación.*

La certificación, una vez concedida, se mantiene de manera indefinida, salvo cambios en las condiciones que motivaron su concesión, tales como avances tecnológicos, aparición de nuevas vulnerabilidades explotables, incumplimiento de las condiciones de uso del certificado, cambios en el propio producto o renuncia expresa del solicitante. Para la

vigilancia de la vigencia de la certificación, el Organismo de Certificación realizará, de oficio, las necesarias auditorías, inspecciones y análisis del producto, de su entorno y del uso del certificado.

### *Sección 2.ª Alcance de la certificación*

**Artículo 113.** *Alcance de la certificación.*

La certificación se limita mediante el correspondiente alcance, que incluye la definición del producto evaluado y las normas y niveles de evaluación.

El Organismo de Certificación, en la determinación del alcance, realizará la definición más precisa posible del mismo, al objeto de evitar confusión alguna entre el producto comercial y el producto evaluado, en el supuesto de que ambos no coincidan exactamente.

**Artículo 114.** *Alcance con relación al producto o sistema evaluado.*

La certificación deberá hacer referencia, e identificar inequívocamente, al producto evaluado, así como a su declaración de seguridad. Dicha declaración de seguridad también deberá contener la identificación precisa del producto evaluado, así como la especificación de su entorno de uso, incluyendo las amenazas previstas, políticas de seguridad e hipótesis aplicables al caso, además de los objetivos de seguridad del producto o sistema y la relación de requisitos de seguridad exigibles al mismo.

Los detalles de la declaración de seguridad podrán variar conforme a las normas aplicadas en la evaluación, pero toda declaración deberá ser un reflejo cierto, claro y preciso de las propiedades de seguridad del producto o sistema evaluado.

**Artículo 115.** *Alcance con relación a las normas y niveles de evaluación.*

La certificación incluirá en su alcance los criterios, métodos y normas de evaluación empleados en la evaluación del producto o sistema, así como el nivel que se haya alcanzado, de los definidos en cada norma, y la relación de interpretaciones e instrucciones técnicas aplicadas.

### *Sección 3.ª Criterios de certificación*

**Artículo 116.** *Informe técnico de evaluación.*

La principal prueba en la instrucción del procedimiento de certificación es el Informe Técnico de Evaluación, emitido por el laboratorio acreditado y realizado cumpliendo con el procedimiento de certificación, establecido en la siguiente Sección.

**Artículo 117.** *Criterios complementarios.*

1. En el ejercicio de su función evaluadora, el Organismo de Certificación podrá, a su criterio, realizar análisis, pruebas, inspecciones y auditorías al laboratorio, al producto a evaluar y al solicitante de la certificación, en los aspectos y requisitos de garantía de seguridad que les sean de aplicación según los criterios y métodos de evaluación utilizados.

2. En particular, será atribución indelegable del Centro Criptológico Nacional el análisis, valoración y acreditación de los algoritmos y medios de cifra que utilice el producto a evaluar.

3. Igualmente, el seguimiento de la evaluación permitirá, al Organismo de Certificación, determinar el ajuste de la evaluación a los procedimientos derivados de las normas aplicables y, por tanto, el ajuste del Informe de Evaluación a las mismas.

### *Sección 4.ª Procedimiento de certificación*

**Artículo 118.** *Proceso de certificación.*

Aquellos interesados que deseen certificar la seguridad de un producto o sistema de Tecnologías de la Información, deberán someterse al proceso establecido en la presente Sección.

**Artículo 119.** *Solicitud de certificación.*

1. La solicitud de certificación deberá remitirse al Director del Organismo de Certificación incluyendo en la misma, como mínimo, la siguiente información debidamente documentada:

a) Personalidad jurídica de la entidad solicitante, con su número de identificación fiscal.
b) Nombre del responsable del solicitante y de la persona, o personas, con capacidad suficiente para obrar, que serán signatarias y, por tanto, responsables de la veracidad de las evidencias y pruebas documentales aportadas.
c) Declaración responsable de conocer y aceptar los términos y requisitos aplicables a la certificación solicitada, incluyendo los derechos de acceso, publicación y limitación de la información de las evaluaciones por parte del Organismo de Certificación.
d) Identificación del laboratorio, acreditado por el Organismo de Certificación, que realizará la evaluación técnica de la seguridad del producto o sistema cuya certificación se solicita.
e) Relación y ubicación de las dependencias, delegaciones e instalaciones donde se realiza la actividad de desarrollo o integración del producto a evaluar.
f) Alcance de la certificación solicitada, indicando el producto a evaluar y su versión, así como las normas y niveles de evaluación aplicables.
g) Justificante del pago de las tasas de certificación en vigor.

Esta solicitud podrá presentarse en cualquiera de los lugares previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. Junto a la solicitud de certificación, se remitirá al Organismo de Certificación la declaración de seguridad, o perfil de protección en su caso, del producto a evaluar y, cuando esto sea posible, una unidad, copia o ejemplar de este último.

3. Paralelamente a la solicitud, el solicitante gestionará con el laboratorio acreditado elegido, el plan detallado de la evaluación, así como el contrato o documento similar que regule las relaciones entre el laboratorio y el solicitante.

**Artículo 120.** *Modelo de solicitud de certificación.*

Las solicitudes de certificación de la seguridad de productos o sistemas de Tecnologías de la Información se presentarán en los impresos establecidos al efecto, que estarán publicados en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es).

**Artículo 121.** *Subsanación y mejora de la solicitud de certificación.*

1. A la recepción de la solicitud de certificación, el Organismo de Certificación realizará una comprobación inicial de la información en ella contenida.

2. En caso de ser necesaria la subsanación o mejora de la solicitud de certificación, se estará a lo dispuesto en el artículo 71 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Se podrá, igualmente, requerir al solicitante el suministro de unidades, copias o ejemplares adicionales del producto a evaluar, conforme a la naturaleza del mismo y a las necesidades derivadas de los criterios complementarios de certificación indicados en el artículo 117.

4. Será obligación del solicitante mantener actualizados el material y la documentación incluidos en la solicitud de certificación, en poder del Organismo de Certificación, en el caso de que alguno de éstos se modifique a resultas del proceso de evaluación correspondiente.

**Artículo 122.** *Notificación al solicitante.*

El Organismo de Certificación notificará al solicitante el inicio del procedimiento administrativo de certificación, incluyendo en dicha notificación el nombre y los datos de contacto del responsable del procedimiento de certificación.

**Artículo 123.** *Aprobación del comienzo de la evaluación.*

1. El laboratorio solicitará, al Organismo de Certificación, la autorización para comenzar la actividad de evaluación. La solicitud irá acompañada de:

a) El plan detallado de la evaluación, con las fases, tareas y unidades de trabajo correspondientes, la asignación e identificación del personal afecto a la evaluación y su responsabilidad en la misma.

b) La copia del contrato o documento similar que regule las relaciones entre el laboratorio y el solicitante de la certificación, en las que el laboratorio incluirá, obligatoriamente, las cláusulas necesarias para el cumplimiento de los requisitos de seguridad para la acreditación del laboratorio.

2. Para la resolución de la solicitud de autorización, se convocará una reunión con el laboratorio a la que asistirá el personal del laboratorio asignado a la evaluación y el equipo de certificación, designado por el Organismo de Certificación.

En esta reunión se harán las presentaciones oportunas y, por parte del laboratorio, se expondrá el plan y calendario de evaluación, así como los aspectos técnicos más relevantes de la misma.

3. El laboratorio deberá demostrar la adecuación y suficiencia de los medios materiales y humanos asignados a la evaluación, en particular, en lo referente a la formación del personal evaluador en los detalles del alcance de la certificación.

4. El Organismo de Certificación resolverá sobre la autorización del comienzo de la actividad de evaluación, incluyendo la designación del responsable del procedimiento de certificación.

**Artículo 124.** *Instrucción de la evaluación.*

1. La instrucción de la evaluación comenzará con el desarrollo de los trabajos de evaluación por parte del laboratorio, durante el cual, el Organismo de Certificación realizará el seguimiento de la actividad de evaluación del producto o sistema cuya certificación se ha solicitado.

Para la realización de este seguimiento, el Organismo de Certificación recibirá, del laboratorio, la información de la evaluación indicada en la Sección 3.ª del Capítulo III, a la vista de la cual convocará las reuniones de seguimiento que considere oportunas. En particular, será de especial atención el ajuste de la ejecución de la evaluación al correspondiente plan de evaluación.

2. La instrucción de la evaluación terminará con el Informe Técnico de Evaluación, que remitirá el laboratorio al Organismo de Certificación, en los siguientes casos:

a) Al término del plazo de evaluación.

b) Por solicitud del Organismo de Certificación. Dicha solicitud se podrá cursar cuando se haya superado, sin subsanar, el plazo de tres meses de cualquier observación o disconformidad, notificada al solicitante de la certificación, o a los tres meses de retraso no justificado del plan de evaluación.

**Artículo 125.** *Informe de certificación.*

El Organismo de Certificación, en un plazo no superior a treinta días contados desde la fecha de la recepción del Informe Técnico de Evaluación, elaborará un informe con los resultados y conclusiones de la evaluación, así como de la actividad de seguimiento, que será enviado al solicitante de la certificación para su conocimiento.

**Artículo 126.** *Audiencia previa a la resolución.*

1. Terminada la instrucción de la evaluación, se pondrá de manifiesto al solicitante de la certificación, convocándole a una reunión de audiencia previa a la resolución.

2. En dicha reunión, el Organismo de Certificación indicará la naturaleza, gravedad y consecuencias de las observaciones y disconformidades, identificadas durante la instrucción del expediente de certificación, si las hubiere, con las implicaciones de las mismas en la resolución de la solicitud de certificación.

3. El solicitante de la certificación, en un plazo no inferior a diez días ni superior a quince, podrá alegar y presentar los documentos y alegaciones que estime pertinentes.

4. Si antes del vencimiento del plazo, el solicitante manifiesta su decisión de no efectuar alegaciones ni aportar nuevos documentos o justificaciones, se tendrá por realizado el trámite.

**Artículo 127.** *Resolución de la solicitud de certificación.*

1. La resolución de la solicitud de certificación se dictará de acuerdo con lo indicado en este artículo, y en los plazos establecidos en el artículo 137, del presente Reglamento.

Esta resolución, de acuerdo con lo previsto en el artículo 116 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, podrá ser objeto de recurso potestativo de reposición ante el Director del Organismo de Certificación, cuya resolución pone fin a la vía administrativa, o ser impugnada directamente ante el orden jurisdiccional contencioso-administrativo.

2. Las resoluciones de desestimación serán motivadas. La resolución de certificación contendrá, adicionalmente, los siguientes extremos:

a) Alcance de la certificación concedida.

b) La fecha de la entrada en vigor de la certificación y referencia a su vigencia.

**Artículo 128.** *Vigencia de la certificación.*

La certificación se concederá por plazo indefinido, salvo cambios en las condiciones que motivaron su concesión, incumplimiento de dichas condiciones o renuncia expresa del solicitante.

Para el mantenimiento de la certificación, el Organismo de Certificación realizará, de oficio, las necesarias revisiones de su vigencia y actividades de vigilancia del uso del certificado, conforme a lo establecido en el artículo 129 siguiente.

**Artículo 129.** *Revisiones de vigencia.*

Cada dos años se realizará una revisión de la vigencia de cada certificado emitido. El objeto de dicha revisión es la comprobación de que el entorno de uso del producto certificado no ha sufrido variaciones, tales como cambios tecnológicos, aparición de vulnerabilidades o cualquier otro aspecto que pueda invalidar las hipótesis, análisis de riesgos y políticas de seguridad reflejadas en dicho entorno de uso.

La revisión de la vigencia de los certificados podrá dar lugar a la anulación del certificado, mediante resolución expresa del Director del Organismo de Certificación.

***Sección 5.ª Seguimiento del uso de los certificados***

**Artículo 130.** *Seguimiento continuo del uso del certificado.*

El Organismo de Certificación realizará un seguimiento continuo del uso de los certificados emitidos, mediante el análisis y registro de toda información comercial o técnica de la que tenga conocimiento y que haga referencia a la certificación emitida.

El incumplimiento de las condiciones de uso del certificado, reguladas en el Capítulo VII, podrá dar lugar a la anulación del certificado, mediante resolución expresa del Director del Organismo de Certificación.

**Artículo 131.** *Ampliación del alcance de la certificación.*

Cuando se desee ampliar el alcance de la certificación de un producto o sistema, el interesado solicitará formalmente dicha ampliación. Para ello deberá utilizar el formulario de solicitud correspondiente. Se aplicará el procedimiento de certificación, indicado en el Capítulo V, adaptado, según proceda, en función del volumen y carácter de dicha ampliación.

**Artículo 132.** *Notificación de cambios.*

El solicitante de la certificación deberá comunicar al Organismo de Certificación los cambios que identifique, relativos al entorno de seguridad del producto certificado, así como cualquier otro cambio fundamental que se produjese en las condiciones iniciales en que se concedió la certificación.

**Artículo 133.** *Publicidad de las certificaciones.*

El Organismo de Certificación podrá hacer pública la relación de productos en proceso de evaluación y la de productos certificados, incluyendo en esta relación la declaración de seguridad de los mismos, así como información derivada del informe de certificación establecido en el artículo 125.

***Sección 6.ª Formulación de observaciones, plazos y recursos***

**Artículo 134.** *Observaciones y retirada de la certificación.*

El incumplimiento, por un solicitante, de las obligaciones derivadas de la certificación dará lugar, en función de la gravedad de la infracción, a la formulación de observaciones o a la retirada de la certificación.

**Artículo 135.** *Actuaciones irregulares e incumplimientos.*

Las actuaciones irregulares y los incumplimientos leves, entendiéndose por tales los que no desvirtúen las restricciones y obligaciones derivadas del uso de la condición de producto certificado, serán objeto de observación, que se notificará, de oficio, al solicitante de la certificación.

El solicitante de la certificación deberá subsanar la causa de tales observaciones en un plazo de diez días.

**Artículo 136.** *Retirada de la certificación.*

1. La disconformidad sostenida, en relación con las restricciones y obligaciones del uso de la condición de producto certificado o con los requisitos para la certificación, así como la falta de subsanación de las observaciones recibidas, darán lugar a la retirada, total o parcial, de la certificación a la que se refiera.

2. La resolución de retirada de certificación se dictará, de oficio, por el Organismo de Certificación.

3. La retirada de la certificación obligará al solicitante al cese inmediato del uso de la condición de producto certificado, en todos los documentos o información en los que la haga manifiesta, y a la retirada del mercado de los productos así etiquetados.

**Artículo 137.** *Plazos y actos presuntos.*

1. El plazo para resolver la solicitud de certificación de productos, y notificar la correspondiente resolución, será de dos meses, contados a partir de la fecha de recepción del Informe Técnico de Evaluación del laboratorio.

Este mismo plazo se aplicará a las solicitudes de ampliación del alcance de una certificación previa.

2. El plazo para resolver la solicitud de comienzo de evaluación, y notificar la correspondiente resolución, será de un mes.

3. A los efectos previstos en el artículo 43 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común, las solicitudes de certificación se entenderán estimadas de no recaer resolución expresa en los plazos establecidos en cada caso, con las salvedades y excepciones indicadas en dicho precepto.

**Artículo 138.** *Recursos.*

La actuación del Organismo de Certificación se atendrá a los principios generales de actuación recogidos en el artículo 3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

De acuerdo con lo previsto en los artículos 116 y 117 de la citada Ley, y en los artículos 10, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, frente a la actuación del Organismo de Certificación, en materia de certificación, los interesados podrán interponer:

a) En el plazo de un mes, recurso potestativo de reposición, ante el Director del dicho organismo, cuya resolución pone fin a la vía administrativa, o

b) Directamente, en el plazo de dos meses, recurso contencioso-administrativo, ante la Sala de dicha índole, del Tribunal Superior de Justicia de Madrid.

## CAPÍTULO VI

## Criterios y metodologías de evaluación

**Artículo 139.** *Estado del arte.*

El Organismo de Certificación certificará la seguridad de los productos y sistemas de Tecnologías de la Información conforme al estado del arte más avanzado en materia de evaluación de la seguridad. Dicho estado del arte se ha de combinar con el debido reconocimiento de los certificados emitidos.

A tal fin, el Organismo de Certificación exigirá a los laboratorios acreditados la realización de su actividad conforme a criterios, métodos y normas bien establecidos y reconocidos. Tales normas se podrán ver complementadas por interpretaciones o instrucciones técnicas emitidas por el Organismo de Certificación.

**Artículo 140.** *Normas de evaluación.*

1. El Organismo de Certificación, a los efectos de su utilización y cumplimiento por parte de los laboratorios, elevará a carácter de norma cualquier documento de orden técnico que sea de su interés, mediante la publicación del mismo en su dirección electrónica (http://www.oc.ccn.cni.es) y su comunicación a los laboratorios acreditados.

2. La publicación de una nueva norma, o la actualización de una existente, y la determinación de su entrada en vigor, se realizarán previa presentación a los laboratorios acreditados de las nuevas normas y de sus diferencias técnicas con respecto a las normas vigentes, a los efectos que pudieran derivarse sobre las acreditaciones en vigor.

3. Las normas relacionadas en el artículo 141 siguiente, se entienden de aplicación en su última versión disponible al comienzo de cada solicitud de certificación. No obstante lo anterior, se podrá consultar la relación de normas, criterios, metodologías y requisitos, así como su aplicabilidad, en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es).

**Artículo 141.** *Criterios de evaluación.*

Los criterios de evaluación serán los recogidos en las siguientes normas:

a) «Common Criteria for Information Technology Security Evaluation» (abreviado, CC).

b) ISO/IEC 15408, «Evaluation Criteria for IT Security».

c) «Information Technology Security Evaluation Criteria» (abreviado, ITSEC). Office for Official Publications of the European Communities.

**Artículo 142.** *Metodologías de evaluación.*

Las metodologías de evaluación serán las recogidas en las siguientes normas:

a) «Common Methodology for Information Technology Security Evaluation» (abreviado, CEM).

b) ISO/IEC 18045, «Methodology for IT Security Evaluation».

c) «Information Technology Security Evaluation Manual» (abreviado, ITSEM). Office for Official Publications of the European Communities.

**Artículo 143.** *Requisitos de seguridad específicos.*

Los requisitos de seguridad específicos serán los recogidos en la norma ISO/IEC 19790, «Requisitos de Seguridad para Módulos Criptográficos».

**Artículo 144.** *Interpretaciones e instrucciones técnicas.*

Se podrá consultar la relación de interpretaciones e instrucciones técnicas en vigor, de aplicación en este Esquema, en la dirección electrónica del Organismo de Certificación (http://www.oc.ccn.cni.es), agrupadas por la norma principal a la que afectan y sus versiones aplicables.

## CAPÍTULO VII

## Uso de la condición de laboratorio acreditado y de producto certificado

**Artículo 145.** *Referencia a la condición de laboratorio acreditado.*

La referencia a la condición de laboratorio acreditado, o el uso del distintivo correspondiente, en los informes emitidos como resultado de las actividades de evaluación amparadas por la acreditación, es el medio por el cual los laboratorios acreditados declaran públicamente el cumplimiento de todos los requisitos de acreditación en la realización de dichas evaluaciones.

Cualquier uso que no esté expresamente permitido en este Reglamento deberá ser consultado al Organismo de Certificación.

**Artículo 146.** *Informes derivados de la evaluación.*

1. La referencia a la condición de laboratorio acreditado debe ser utilizada en todos los informes emitidos como resultado de las actividades de evaluación, amparadas por la acreditación, como garantía del cumplimiento de los requisitos de dicha acreditación.

2. Cualquier informe o certificado que no incluya la referencia a la condición de laboratorio acreditado, no garantiza el cumplimiento de los requisitos de acreditación y, por tanto, no será aceptado por el Organismo de Certificación, como parte de una evaluación acreditada, ni podrá beneficiarse del reconocimiento de los certificados emitidos por el Organismo de Certificación.

3. En el caso de informes que incluyan, tanto datos amparados por la acreditación, como datos no amparados por la misma, se seguirán las siguientes reglas:

a) Se señalarán los datos no amparados por la acreditación mediante la utilización de un asterisco o similar. Asimismo, se deberá incluir en un lugar visible la siguiente leyenda: «Los ensayos/inspecciones marcados no están incluidos en el alcance de acreditación».

b) Cuando un informe de evaluación contenga interpretaciones, opiniones o cualquier otra información relativa a investigación, que no sea parte de la metodología de ensayo seguida en esa evaluación, se deberá incluir la siguiente advertencia: «Las opiniones, interpretaciones, etc., que se indican a continuación, están fuera del alcance de la acreditación del Organismo de Certificación».

**Artículo 147.** *Otros documentos de laboratorio acreditado.*

En documentos de tipo publicitario, folletos o anuncios relacionados con la actividad de evaluación acreditada, o en material de papelería (papel de cartas, impresos tales como facturas o pedidos, sobres, etc.), los laboratorios podrán usar la referencia a la condición de acreditado con las restricciones que se mencionan en el artículo 148.

**Artículo 148.** *Restricciones al uso de la condición de laboratorio acreditado.*

La referencia a la condición de laboratorio acreditado no se debe utilizar en los siguientes supuestos:

a) En informes o certificados que no contengan ningún dato obtenido de actividades acreditadas.

b) En documentos en los que no se identifique la organización a la que ha sido concedida la acreditación.

c) De forma que pueda sugerir que el Organismo de Certificación aprueba, acepta o, de alguna manera, se responsabiliza de los resultados contenidos en un informe o certificado (por ejemplo, mediante el uso de sellos con la referencia al Organismo de Certificación).

d) Cuando el laboratorio haya perdido su condición de acreditado, ya sea de forma voluntaria o por retirada de la acreditación.

e) En las tarjetas de visita del personal de los laboratorios acreditados.

f) En cualquier situación que pueda dar lugar a una interpretación incorrecta de la condición del laboratorio acreditado, o que pueda inducir a considerar actividades no acreditadas como cubiertas por la acreditación. Concretamente:

1.º Cuando se use en impresos (ofertas, cartas, presentaciones comerciales, material publicitario, páginas Web, etc.), que hagan referencia a actividades no acreditadas, se deberá incluir una mención, con el mismo tamaño de letra que el usado en el cuerpo del documento en cuestión, en la que se aclare este hecho (por ejemplo: «Las actividades recogidas en el presente escrito no están incluidas en el alcance de la acreditación del Organismo de Certificación»).

2.º Cuando se use en impresos (ofertas, cartas, presentaciones comerciales, material publicitario, etc.), que incluyan tanto actividades acreditadas como no acreditadas, su uso deberá ser tal, que permita al lector distinguir aquellas actividades que están acreditadas de las que no lo están.

3.º Cuando un laboratorio esté compuesto por varios emplazamientos distintos, y no todos ellos hayan sido acreditados, solamente aquellos que sí lo hayan sido podrán hacer uso de la referencia a la condición de acreditado. Cuando se emitan documentos comunes a todo el laboratorio se deberá incluir una cláusula que indique esta condición (por ejemplo: «Se encuentra disponible la lista de emplazamientos acreditados y sus alcances»).

4.º Cuando una organización acreditada pertenezca a otra mayor, no deberá existir confusión sobre cual de ellas está acreditada.

g) En cualquier otro supuesto que resulte abusivo, a juicio del Organismo de Certificación.

**Artículo 149.** *Uso de la condición de producto certificado.*

El uso del distintivo especificado en el artículo 155, o la referencia a la condición de producto certificado, es el medio por el cual los solicitantes de la certificación declaran, públicamente, el cumplimiento de todos los requisitos exigibles para dicha certificación, la conformidad con determinados perfiles de protección, en su caso, y el cumplimiento de las disposiciones legales aplicables.

Cualquier uso del certificado que no esté expresamente permitido en este Reglamento, deberá ser consultado al Organismo de Certificación.

**Artículo 150.** *Producto y documentación.*

La referencia a la condición de producto certificado debe ser utilizada en toda la documentación de administración y uso de dicho producto, y que se haya remitido como evidencia de la evaluación.

La referencia a la condición de producto certificado se incluirá también en el propio producto, siguiendo las reglas de marcado indicadas en el artículo 155.

**Artículo 151.** *Otros documentos de producto certificado.*

En documentos de tipo publicitario, folletos o anuncios relacionados con el producto certificado, así como en los contratos públicos y privados, licitaciones y documentación preparatoria, el titular de la certificación podrá usar la referencia a la condición de producto certificado con las restricciones que se mencionan en el artículo 152.

**Artículo 152.** *Restricciones al uso de la condición de producto certificado.*

La referencia a la condición de producto certificado no debe utilizarse en los siguientes supuestos:

a) Sin una referencia completa e inequívoca del alcance del certificado. Como mínimo se citará:

1.º Nombre y versión del producto evaluado.
2.º La norma utilizada para la evaluación y el nivel alcanzado en la misma (por ejemplo: ISO/IEC 15408 EAL2).
3.º Referencia a la declaración de seguridad del producto certificado, indicando el procedimiento para obtener una copia de la misma.

b) De forma que pueda sugerir que el certificado se aplica a todo un sistema o producto, cuando el producto evaluado es sólo una parte del mismo.
c) De forma que se sugieran propiedades de seguridad del producto certificado no reflejadas en su declaración de seguridad.
d) Cuando el certificado haya sido anulado por cualquier motivo.
e) En cualquier otro uso que resulte abusivo a juicio del Organismo de Certificación.

**Artículo 153.** *Otras obligaciones de la condición de producto certificado.*

La referencia a la condición de producto certificado obligará al solicitante de la certificación a:

a) Mantener registro de todas las reclamaciones presentadas al solicitante, relativas a la seguridad del producto certificado, y a tener esta información disponible para el Organismo de Certificación.
b) Tomar las acciones correctoras apropiadas con respecto a tales reclamaciones y a cualquier deficiencia encontrada en los productos, que afecten la conformidad con los requisitos para la certificación.
c) Documentar las acciones tomadas.

**Artículo 154.** *Distintivo de laboratorio acreditado.*

La condición de laboratorio acreditado puede complementarse mediante el uso del distintivo descrito a continuación (figura 2):

a) Color de fondo, diseño y detalles del escudo y tipo de letra, conforme a lo dispuesto en el Real Decreto 1465/1999, de 17 de septiembre, que establece los criterios de imagen institucional y regula la producción documental y el material impreso de la Administración General del Estado, y en la Orden de 27 de septiembre de 1999 por la que se aprueba el Manual de Imagen Institucional de la Administración General del Estado y se dictan normas de desarrollo del Real Decreto 1465/1999 citado (consultar página web «http://www.060.es»).
b) Círculo exterior de 180 unidades de medida de diámetro. Tamaño de letra nueve veces inferior al radio, esto es, de 20 unidades de medida.
c) Leyenda exterior, «ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD TI», sobre un arco de 270 grados, 140 unidades de medida de radio, y ángulo inicial de 135 grados, sentido negativo del texto.
d) Leyenda interior, «LABORATORIO ACREDITADO», sobre un arco de radio de 100 unidades de medida, iguales ángulos y recorrido que el exterior.
e) Escudo de España equidistante en sus aristas a la leyenda interior.
f) Si se reduce o amplía el distintivo, deberán respetarse las proporciones de este modelo.
g) La altura del distintivo no será inferior a 15 mm.


Figura 2. Distintivo de laboratorio acreditado

**Artículo 155.** *Distintivo de producto certificado.*

Los productos certificados deberán llevar un distintivo conforme a lo siguiente (figura 3):

a) Color de fondo, diseño y detalles del escudo y tipo de letra, conforme a lo dispuesto en el Real Decreto 1465/1999, de 17 de septiembre, que establece los criterios de imagen institucional y regula la producción documental y el material impreso de la Administración General del Estado, y en la Orden de 27 de septiembre de 1999 por la que se aprueba el Manual de Imagen Institucional de la Administración General del Estado y se dictan normas de desarrollo del Real Decreto 1465/1999 citado (consultar página web «http://www.060.es»).

b) Círculo exterior de 180 unidades de medida de diámetro. Tamaño de letra nueve veces inferior al radio, esto es, de 20 unidades de medida.

c) Leyenda exterior, «ESQUEMA DE EVALUACIÓN Y CERTIFICACIÓN DE LA SEGURIDAD TI», sobre un arco de 270 grados, 140 unidades de medida de radio, y ángulo inicial de 135 grados, sentido negativo del texto.

d) Leyenda interior, «PRODUCTO CERTIFICADO», sobre un arco de radio de 100 unidades de medida, iguales ángulos y recorrido que el exterior.

e) Escudo de España equidistante en sus aristas a la leyenda interior.

f) Si se reduce o amplía el distintivo, deberán respetarse las proporciones de este modelo.

g) La altura del distintivo no será inferior a 15 mm, excepto cuando esto no sea posible a causa del tipo de producto.


Figura 2. Distintivo de producto certificado con indicación del alcance

h) El distintivo deberá colocarse en el producto o en su placa informativa. Además, deberá colocarse en el embalaje, si existe, y en la documentación que le acompañe. En productos software, se mostrará el distintivo donde se haga referencia a la versión particular del producto.

i) El distintivo deberá colocarse de forma visible, legible e indeleble.

j) Se incluirá un elemento destinado a informar al usuario sobre el alcance de la certificación (norma y nivel aplicados en la evaluación).

# § 36

## Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 77, de 31 de marzo de 2021
Última modificación: 12 de julio de 2022
Referencia: BOE-A-2021-5032

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, consagran el derecho de las personas a relacionarse por medios electrónicos con las administraciones públicas, simplificando el acceso a los mismos, y refuerzan el empleo de las tecnologías de la información y las comunicaciones (TIC) en las administraciones públicas, tanto para mejorar la eficiencia de su gestión como para potenciar y favorecer las relaciones de colaboración y cooperación entre ellas.

Ambas leyes recogen los elementos que conforman el marco jurídico para el funcionamiento electrónico de las Administraciones Públicas introduciendo un nuevo paradigma que supera la concepción que inspiró la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y su desarrollo reglamentario parcial en la Administración General del Estado y sus organismos públicos vinculados o dependientes a través del Real Decreto 1671/2009, de 6 de noviembre, según la cual la tramitación electrónica no era sino una forma de gestión de los procedimientos.

En este sentido, la Ley 11/2007, de 22 de junio, respondiendo a las nuevas realidades, exigencias y experiencias que se habían puesto de manifiesto, al propio desarrollo de la sociedad de la información y al cambio de circunstancias tecnológicas y sociales, entre otros factores, reconocía el derecho de la ciudadanía a relacionarse electrónicamente con las Administraciones Públicas, y no solo la posibilidad como se preveía en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La Ley 11/2007, de 22 de junio admitía incluso que, por vía reglamentaria, se estableciese la obligatoriedad de comunicarse con las Administraciones Públicas por medios electrónicos cuando las personas interesadas fuesen personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tuviesen garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

En este contexto, la Ley 39/2015, de 1 de octubre, y la Ley 40/2015, de 1 de octubre, han dado respuesta a la demanda actual en el sentido de que la tramitación electrónica de los procedimientos debe constituir la actuación habitual de las Administraciones Públicas, y no solamente ser una forma especial de gestión de los mismos. En consecuencia, se prevé que las relaciones de las Administraciones entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes se realizará a través de medios electrónicos, y se

establece la obligatoriedad de relacionarse electrónicamente con la Administración para las personas jurídicas, entes sin personalidad y, en algunos supuestos, para las personas físicas, y ello sin perjuicio de la posibilidad de extender esta obligación a otros colectivos, por vía reglamentaria.

Con estos antecedentes, era necesario desarrollar y concretar las previsiones legales con el fin, entre otros aspectos, de facilitar a los agentes involucrados en el uso de medios tecnológicos su utilización efectiva, aclarando y precisando, al mismo tiempo, aquellas materias reguladas en estas leyes que permiten un margen de actuación reglamentaria.

La satisfacción del interesado, por tanto, en el uso de los servicios públicos digitales es fundamental para garantizar adecuadamente sus derechos y el cumplimiento de sus obligaciones en su relación con las Administraciones Públicas. Por ello, es prioritario disponer de servicios digitales fácilmente utilizables y accesibles, de modo que se pueda conseguir que la relación del interesado con la Administración a través del canal electrónico sea fácil, intuitiva, efectiva, eficiente y no discriminatoria.

Por otra parte, a lo largo de las dos últimas décadas, los sucesivos Gobiernos de España han ido adoptando programas para el avance digital alineados con las agendas digitales europeas, en todos los cuales ha estado presente el eje de mejora de la Administración electrónica. Fruto de estos programas, España cuenta con una posición muy favorable para abordar la siguiente fase del proceso de Transformación digital de nuestro país y, en lo que concierne a la Administración electrónica, está situada entre los países más avanzados de la Unión Europea, lo que se ha logrado gracias al esfuerzo continuado de las Administraciones Públicas en la adaptación de sus servicios electrónicos para ofrecer cada vez mejores servicios, más adaptados a las demandas de la ciudadanía y las empresas, y más eficientes. En este esfuerzo, la estrategia de España se ha basado en el impulso de los fundamentos que permiten una tramitación electrónica completa, y en el desarrollo de servicios que pueden ser utilizados libremente por todas las Administraciones Públicas, y que están alineados con los esquemas de interoperabilidad europeos.

Los cambios que se están produciendo con la maduración de tecnologías disruptivas y su aplicación a la gestión de la información y la ejecución de políticas públicas, los nuevos modelos de relación de la ciudadanía y empresas con las Administraciones y la reutilización eficiente de la información son grandes desafíos que para ser afrontados con éxito y para que coadyuven a la Transformación digital exigen como presupuesto contar con un marco regulatorio adecuado, tanto con rango de ley como con rango reglamentario, que garantizando la seguridad jurídica para todos los intervinientes sirva a los objetivos de mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada, incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica y garantizar servicios digitales fácilmente utilizables.

En este sentido, la Agenda España Digital 2025 contiene un eje estratégico específico sobre la Transformación Digital del Sector Público, cuya plasmación se concreta en el cumplimiento de un conjunto de medidas entre las que se encuentra la mejora del marco regulatorio de la Administración digital y específicamente en la aprobación de este real decreto. Por su parte, el Plan de Recuperación, Transformación y Resiliencia (España Puede) incluye entre sus diez políticas palanca de reforma estructural para un crecimiento sostenible e inclusivo, lograr una Administración modernizada a través de su digitalización, tanto a nivel transversal como en ámbitos estratégicos, que actúe como tractor de los cambios tecnológicos. El último hito en estrategia transformadora lo constituye el Plan de Digitalización de las Administraciones Públicas 2021 -2025, que supone un salto decisivo en la mejora de la eficacia y eficiencia de la Administración Pública, en la transparencia y eliminación de trabas administrativas a través de la automatización de la gestión, en una mayor orientación a la personalización de servicios y a la experiencia de usuario, actuando todo ello de elemento catalizador de la innovación tecnológica de nuestro país desde el ámbito público.

En definitiva, el Reglamento que aprueba este real decreto persigue los cuatro grandes objetivos mencionados: mejorar la eficiencia administrativa, incrementar la transparencia y la participación, garantizar servicios digitales fácilmente utilizables y mejorar la seguridad jurídica.

En primer lugar, persigue mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada. Así, se desarrolla y concreta el empleo de los medios electrónicos establecidos en las leyes 39/2015, de 1 de octubre, y 40/2015, de 1 de octubre, para garantizar, por una parte, que los procedimientos administrativos se tramiten electrónicamente por la Administración y, por otra, que la ciudadanía se relacione con ella por estos medios en los supuestos en que sea establecido con carácter obligatorio o aquellos lo decidan voluntariamente.

Un segundo objetivo consiste en incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica. Así, se desarrolla el funcionamiento del Punto de Acceso General electrónico (PAGe), y la Carpeta ciudadana en el Sector Público Estatal. Se regula el contenido y los servicios mínimos a prestar por las sedes electrónicas y sedes electrónicas asociadas y el funcionamiento de los registros electrónicos.

En tercer lugar, el Reglamento persigue garantizar servicios digitales fácilmente utilizables de modo que se pueda conseguir que la relación del interesado con la Administración sea fácil, intuitiva y efectiva cuando use el canal electrónico.

Por último, busca mejorar la seguridad jurídica. Así, se elimina la superposición de regímenes jurídicos distintos, se adapta e integra en el Reglamento que aprueba este real decreto la regulación que aún permanecía vigente del Real Decreto 1671/2009, de 6 de noviembre, procediendo, por ello, a su derogación definitiva y se adecua la regulación al nuevo marco de la Ley 39/2015, de 1 de octubre y la Ley 40/2015, de 1 de octubre.

El real decreto consta de un artículo único que aprueba el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos, dos disposiciones transitorias, una disposición derogatoria y cinco disposiciones finales.

Entre las cinco disposiciones finales hay dos que modifican normas vigentes y las tres restantes regulan el título competencial, la habilitación reglamentaria para el desarrollo y ejecución del real decreto y la entrada en vigor. Respecto de las disposiciones modificativas, estas afectan al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y al Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Así, en primer lugar, con relación al Real Decreto 4/2010, de 8 de enero, su artículo 29 establece que el Esquema Nacional de Interoperabilidad se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de Administración electrónica, la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que lo apoyan. Por ello, la rápida evolución de las tecnologías, la experiencia derivada de la aplicación del Esquema Nacional de Interoperabilidad desde su aprobación hace 10 años, las previsiones de la Ley 39/2015, de 1 de octubre, y de la Ley 40/2015, de 1 de octubre, relativas a la interoperabilidad entre las Administraciones Públicas y sus órganos, organismos públicos y entidades de derecho público vinculados o dependientes, más la necesidad de adecuarse a lo previsto en el Reglamento n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión no 1673/2006/CE del Parlamento Europeo y del Consejo, determinan la necesidad de proceder a modificar ciertos aspectos de su redacción actual. En consecuencia, se modifican los artículos, 9, 11, 14, 16, 17, y 18, así como la disposición adicional primera y el anexo de glosario, a la vez que se suprimen el artículo 19 y las disposiciones adicionales tercera y cuarta.

En segundo lugar, se modifica el Real Decreto 931/2017, de 27 de octubre, para incorporar en la Memoria del Análisis de Impacto Normativo el análisis de la incidencia en los gastos en medios o servicios de la Administración digital dentro del impacto presupuestario de los proyectos y, por otra parte, para incluir dentro del apartado de «Otros impactos» el que tendrá para las personas destinatarias de la norma y para la organización y funcionamiento de la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la aplicación de la normativa proyectada.

Por su parte, el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos que aprueba el real decreto consta de 65 artículos distribuidos en cuatro títulos, diez disposiciones adicionales y un anexo de definiciones.

El título preliminar del Reglamento comprende las disposiciones generales regulando el objeto y ámbito de aplicación de la norma (que se remite al ámbito del artículo 2 tanto de la Ley 39/2015, de 1 de octubre, como de la Ley 40/2015, de 1 de octubre) y los principios generales que debe respetar el sector público en sus actuaciones y relaciones electrónicas. Entre estos principios se incluyen el de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías y sistemas de comunicaciones electrónicas, para garantizar tanto la independencia en la elección de las alternativas tecnológicas necesarias para relacionarse con las Administraciones Públicas por parte de las personas interesadas y por el propio sector público, como la libertad para desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado; el principio de accesibilidad, para promover que el diseño de los servicios electrónicos garantice la igualdad y no discriminación en el acceso de las personas usuarias, en particular, de las personas discapacitadas y de las personas mayores; el principio de facilidad de uso, que determina que el diseño de los servicios electrónicos esté centrado en las personas usuarias para minimizar el grado de conocimiento tecnológico necesario para el uso del servicio, el principio de interoperabilidad, entendido como la capacidad de los sistemas de información y,por ende, de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos; el principio de proporcionalidad, para que las medidas de seguridad y garantías que se exijan sean adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos y, por último, el principio de personalización y proactividad, entendido como la capacidad de las Administraciones Públicas para que, partiendo del conocimiento adquirido del usuario final del servicio, proporcione servicios precumplimentados y se anticipe a las posibles necesidades de los mismos.

Asimismo el título preliminar regula el derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas, en aplicación del artículo 14 de la Ley 39/2015, de 1 de octubre, y los canales a través de los cuales las Administraciones Públicas prestarán la asistencia necesaria para facilitar el acceso de las personas interesadas a los servicios electrónicos proporcionados en su ámbito.

El título I regula los portales de internet, el PAGe, las sedes electrónicas y sedes electrónicas asociadas (características, creación y supresión, contenido y servicios, y responsabilidad) y el área personalizada a través de la cual cada interesado podrá acceder a su información, al seguimiento de los trámites administrativos que le afecten y a las notificaciones y comunicaciones en el ámbito de la Administración Pública competente, que en el ámbito estatal se denomina «Carpeta Ciudadana».

El título II se subdivide en tres capítulos y regula el procedimiento administrativo por medios electrónicos. Así, el capítulo I, sobre «Disposiciones generales» aborda la tramitación administrativa automatizada y el régimen de subsanaciones. Por su parte el capítulo II regula la identificación y autenticación de las Administraciones Públicas y de las personas interesadas y se subdivide en cuatro Secciones: la 1ª aborda las disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad (incluyendo la plataforma de verificación de certificados electrónicos y otros sistemas de identificación), la 2.ª regula la «Identificación electrónica de las Administraciones Públicas y la autenticación del ejercicio de su competencia», que comprende la identificación de las sedes electrónicas y sedes asociadas, la identificación mediante sello electrónico basado en certificado electrónico cualificado, los sistemas de firma electrónica para la actuación administrativa automatizada, la identificación y firma del personal al servicio de las Administraciones Públicas (incluidos los certificados de empleado público con número de identificación profesional) y la autenticación e identificación de las Administraciones emisoras y receptoras en intercambio de datos a través de entornos cerrados de comunicación. La sección 3ª desarrolla la regulación de la identificación y firma de las personas interesadas y, por último, la sección 4ª regula la acreditación de la representación de las personas interesadas (regulando, entre otros extremos, el registro electrónico de apoderamientos).

El título II se cierra con el capítulo III, que en sus dos secciones regula los Registros electrónicos, las notificaciones electrónicas y los otros actos de comunicación electrónicos.

Así, la sección 1ª regula los registros electrónicos (entre otros aspectos, el Registro Electrónico General de cada Administración y la presentación y tratamiento de documentos en registro o las competencias de las Oficinas de asistencia en materia de registros de la Administración General del Estado) y la sección 2ª regula las comunicaciones administrativas a las personas interesadas por medios electrónicos (actos de comunicación electrónica a las personas interesadas distintos de las notificaciones o publicaciones) y las notificaciones electrónicas (incluyendo las reglas generales de la práctica de las notificaciones electrónicas, el aviso de puesta a disposición de la notificación, la notificación a través de la Dirección Electrónica Habilitada única (DEHu) y la notificación electrónica en sede electrónica o sede electrónica asociada).

El título III regula el expediente electrónico y se divide en dos capítulos. El capítulo I regula el documento administrativo electrónico y los requisitos y la emisión de copias auténticas de documentos públicos administrativos o documentos privados, que sean originales o copias auténticas de originales; la formación del expediente administrativo electrónico y el ejercicio de acceso al mismo y a la obtención de copias y la destrucción de documentos. Por su parte, el capítulo II regula la conservación de documentos electrónicos y la definición de archivo electrónico único.

Por último, el título IV se divide en dos capítulos y regula las relaciones y colaboración entre Administraciones Públicas para el funcionamiento electrónico del sector público. Así, el capítulo I aborda la colaboración entre las Administraciones Públicas para la actuación administrativa por medios electrónicos e incluye las obligadas relaciones interadministrativas e interorgánicas por medios electrónicos en el ejercicio de sus competencias, las comunicaciones en la Administración General del Estado, la posibilidad de adhesión a sedes electrónicas y sedes electrónicas asociadas y la regulación del Sistema de Interconexión de Registros (SIR), a través del cual deberán realizarse las interconexiones entre Registros de las Administraciones Públicas, que deberán ser interoperables entre sí y, en el caso de la Administración General del Estado, lo que supone una novedad, también con los sistemas de gestión de expedientes.

El capítulo I del título IV regula también las transmisiones de datos a las que se refiere el artículo 155 de la Ley 40/2015 de 1 de octubre, las plataformas de intermediación de datos (con mención especial a la de ámbito estatal), la remisión electrónica de expedientes administrativos en el ámbito de las Administraciones públicas mediante puesta a disposición, a través de un nodo de interoperabilidad, de la dirección electrónica o localizador que dé acceso al expediente electrónico completo y, por último, las previsiones el intercambio automático de datos o documentos a nivel europeo previstos en el Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.º 1024/2012.

El título IV finaliza con el capítulo II, que regula la transferencia y uso compartido de tecnologías entre Administraciones Públicas, abordando, por una parte, la reutilización de sistemas y aplicaciones de las Administraciones Públicas y, por otra, la adhesión a las plataformas, registros o servicios electrónicos de la Administración General del Estado

La parte final del Reglamento consta de diez disposiciones adicionales y un anexo de definiciones. Las primeras regulan la obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado; la promoción de la formación del personal al servicio de la Administración General del Estado para garantizar el derecho de las personas interesadas a ser asistidas en el uso de medios electrónicos en sus relaciones con la Administración Pública; la creación del nodo de interoperabilidad para la identificación electrónica del Reino de España para el reconocimiento mutuo de identidades electrónicas entre Estados miembros de la Unión Europea; la adhesión de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado, en el ejercicio de potestades administrativas, a las sedes electrónicas y sedes electrónicas asociadas y sistema de firma y notificaciones electrónicas aplicables; la adhesión de los órganos constitucionales al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado; la situación de las sedes electrónicas y subsedes electrónicas en el ámbito estatal existentes a

la entrada en vigor de este real decreto; la interoperabilidad de los registros electrónicos de apoderamientos; supletoriedad en Registro Civil; la autorización de los sistemas de identificación previstos en el artículo 9.2.c) y de los sistemas de firma previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre y, por último, las especialidades por razón de materia.

El Reglamento concluye con un Anexo terminológico que retoma la buena praxis que incluía la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en una materia de especial complejidad por la imbricación de categorías jurídicas y conceptos tecnológicos en permanente evolución.

El real decreto se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia), en tanto que persigue un interés general al concretar determinados aspectos de la Ley 39/2015, de 1 de octubre y de la Ley 40/2015, de 1 de octubre, que van a facilitar el uso efectivo de los medios electrónicos de la Administración, y el desarrollo necesario de las citadas leyes. La norma es acorde con el principio de proporcionalidad al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento jurídico, estableciéndose un marco normativo estable, integrado y claro. Asimismo, durante el procedimiento de elaboración de la norma, se han formalizado los trámites de consulta pública previa e información pública, que establece la Ley en cumplimiento del principio de transparencia, quedando además justificados en el preámbulo los objetivos que persigue este real decreto. Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación, en materia de cargas administrativas, respecto de las leyes que con esta norma se desarrollan.

Asimismo, el proyecto ha sido informado por la Agencia Española de Protección de Datos y se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y a informe de los diferentes ministerios.

El real decreto se dicta en ejercicio de la habilitación normativa contenida en la disposición final sexta de la Ley 39/2015, de 1 de octubre, y en la disposición final decimoquinta de la Ley 40/2015, de 1 de octubre, para llevar a cabo su desarrollo reglamentario en lo referido a la gestión electrónica de los procedimientos y el funcionamiento electrónico del sector público y garantizar, así, la efectiva aplicación e implantación de las previsiones que ambas leyes establecen, todo ello al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución. Los artículos 15,16, 23, 26, 28.2, 28.3 y 29.4 y la disposición adicional tercera del Reglamento, en cuanto a su relación con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, además, de acuerdo con lo dispuesto en los artículos 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital y del Ministro de Política Territorial y Función Pública, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 30 de marzo de 2021,

DISPONGO:

**Artículo único.** *Aprobación del Reglamento de actuación y funcionamiento del sector público por medios electrónicos.*

Se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, cuyo texto se incluye a continuación.

**Disposición transitoria primera.** *Destrucción de documentos en soporte no electrónico.*

**(Anulada)**

**Disposición transitoria segunda.** *Portales de internet existentes y aplicaciones específicas en el ámbito estatal.*

1. La supresión de los portales de internet creados en el ámbito estatal antes de la entrada en vigor de este real decreto se regirá por las reglas aplicables en el momento de su creación.

2. En el plazo de seis meses desde la entrada en vigor de este real decreto, en el ámbito de cada ministerio se analizará la oportunidad del mantenimiento de sus portales de internet existentes y los de sus organismos públicos o entidades de derecho público vinculados o dependientes respectivos, así como de las páginas web promocionales («microsites»). Para ese análisis se aplicarán los mismos criterios previstos en el artículo 6 para la creación de nuevos portales y se decidirá acerca de su mantenimiento o su supresión.

En caso de que se decida la supresión, se valorará si es pertinente o no incorporar en el PAGe de la Administración General del Estado la información que se ha contenido en dichos portales hasta la supresión.

3. Realizado el proceso previsto en el apartado anterior, en el plazo máximo de un año desde la entrada en vigor de este real decreto se publicará en el PAGe de la Administración General del Estado una Resolución del Secretario General de Función Pública, en la que figurará el listado de portales de internet activos de la Administración General del Estado y de los organismos públicos o entidades de derecho público vinculados o dependientes de esta.

4. En el plazo máximo de un año desde la entrada en vigor de este real decreto, y a partir de la información facilitada por los ministerios, la Secretaría General de Administración Digital realizará el censo de aplicaciones específicas diseñadas para dispositivos móviles («app») para su utilización en los procedimientos de la Administración General del Estado.

5. En el ámbito de la Administración General del Estado, los portales de internet muy reconocidos e identificables por los usuarios, creados antes de la entrada en vigor de este real decreto se regirán por las reglas aplicables en el momento de su creación en cuanto a nomenclatura, sin necesidad de que modifiquen el nombre del dominio de segundo nivel.

**Disposición derogatoria única.** *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto y, en concreto, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

**Disposición final primera.** *Títulos competenciales.*

1. Este real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de procedimiento administrativo común y para dictar las bases del régimen jurídico de las Administraciones Públicas.

2. Los artículos 15, 16, 23, 26, 28.2, 28.3 y 29.4 y la disposición adicional tercera del Reglamento que aprueba este real decreto, en cuanto a su relación con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, además, de acuerdo con lo dispuesto en los artículos 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente.

3. No tiene carácter básico y será de aplicación únicamente en el ámbito estatal lo dispuesto en:

a) La disposición transitoria segunda y la disposición final tercera de este real decreto.

b) El segundo párrafo del apartado 3 del artículo 3, los artículos 6, 7.4, 8, 10.3, 10.4, 13.2, 17, 18.2, 19.3, 19.4, 21.4, 23.2, 24, 25.4, 28.3, 30.2, 31, 33, 36, 38.1, el segundo párrafo del apartado 4 del artículo 39, los artículos 40, 42.5, 48, 53.5, 55.2, 57, 60.3, 62.2 y las disposiciones adicionales primera, segunda, cuarta, quinta, sexta, el segundo apartado de la disposición adicional séptima del Reglamento que aprueba este real decreto.

**Disposición final segunda.** *Modificación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.*

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica queda modificado como sigue:

Uno. El artículo 9 queda redactado del siguiente modo:

**«Artículo 9.** *Inventarios de información administrativa.*

1. Cada Administración Pública mantendrá actualizado el conjunto de sus inventarios de información administrativa que incluirá, al menos:

a) La relación de los procedimientos administrativos y servicios prestados de forma clasificada y estructurada. Las Administraciones Públicas conectarán electrónicamente sus inventarios con el Sistema de Información Administrativa gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital.

b) La relación de sus órganos administrativos y oficinas orientadas al público y sus relaciones entre ellos. Dicho inventario se conectará electrónicamente con el Directorio Común de Unidades Orgánicas y Oficinas, gestionado por el Ministerio de Asuntos Económicos y Transformación Digital, en colaboración con el Ministerio de Política Territorial y Función Pública, que proveerá una codificación unívoca.

2. Cada Administración Pública regulará la creación y mantenimiento de estos dos inventarios, en las condiciones que se determinen, con carácter general, por las normas técnicas de interoperabilidad correspondientes; en su caso, las Administraciones Públicas podrán hacer uso de los citados Sistema de Información Administrativa y Directorio Común de Unidades Orgánicas y Oficinas para la creación y mantenimiento de sus propios inventarios. Para la descripción y modelización de los procedimientos administrativos y de los procesos que los soportan será de aplicación lo previsto sobre estándares en el artículo 11.»

Dos. El párrafo a) del artículo 11.3, queda redactado como sigue:

«a) El uso de las especificaciones técnicas de las TIC en la contratación pública junto con las definiciones de norma y especificación técnica establecidos en el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea.»

Tres. Se modifica el artículo 14, que queda redactado como sigue:

**«Artículo 14.** *Plan de direccionamiento de la Administración.*

Las Administraciones Públicas aplicarán el Plan de direccionamiento e interconexión de redes en la Administración, desarrollado en la norma técnica de interoperabilidad correspondiente, para su interconexión a través de las redes de comunicaciones.»

Cuatro. Se modifica el artículo 16, que queda redactado como sigue:

**«Artículo 16.** *Condiciones de licenciamiento aplicables.*

1. Las condiciones de licenciamiento de las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información cuya titularidad de los derechos de la propiedad intelectual sea de una Administración Pública y permita su puesta a disposición de otra Administración y de los ciudadanos tendrán en cuenta los siguientes aspectos:

a) El fin perseguido es el aprovechamiento y la reutilización de recursos públicos.

b) La completa protección contra su apropiación exclusiva o parcial por parte de terceros.

c) La exención de responsabilidad del cedente por el posible mal uso por parte del cesionario.

d) La no obligación de asistencia técnica o de mantenimiento por parte del cedente.

e) La ausencia total de responsabilidad por parte del cedente con respecto al cesionario en caso de errores o mal funcionamiento de la aplicación.

f) El licenciamiento se realizará por defecto sin contraprestación y sin necesidad de establecer convenio alguno. Sólo se podrá acordar la repercusión parcial del coste de adquisición o desarrollo de las aplicaciones cedidas en aquellos casos en los que este pago repercuta directamente en el incremento de funcionalidades del activo cedido, incluya adaptaciones concretas para su uso en el organismo cesionario, o impliquen el suministro de servicios de asistencia o soporte para su reutilización en el organismo cesionario.

2. Las Administraciones Públicas utilizarán para las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información declarados como de fuentes abiertas aquellas licencias que aseguren que los programas, datos o información cumplen los siguientes requisitos:

a) Pueden ejecutarse para cualquier propósito.

b) Permiten conocer su código fuente.

c) Pueden modificarse o mejorarse.

d) Pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas cuatro garantías.

3. Para este fin se procurará la aplicación de la Licencia Pública de la Unión Europea, sin perjuicio de otras licencias que garanticen los mismos derechos expuestos en los apartados 1 y 2.

4. A efectos de facilitar el establecimiento de las condiciones de licenciamiento, las Administraciones Públicas incluirán en los pliegos de cláusulas técnicas de aquellos contratos que tengan por finalidad el desarrollo de nuevas aplicaciones informáticas, los siguientes aspectos:

a) Que la Administración contratante adquiera los derechos completos de propiedad intelectual de las aplicaciones y cualquier otro objeto de información que se desarrollen como objeto de ese contrato.

b) Que en el caso de reutilizar activos previamente existentes, la Administración contratante reciba un producto que pueda ofrecer para su reutilización posterior a otras Administraciones Públicas. Además, en el caso de partir de productos de fuentes abiertas, que sea posible declarar como de fuentes abiertas la futura aplicación desarrollada.»

Cinco. Se modifica el artículo 17, que queda redactado como sigue:

**«Artículo 17.** *Directorios de aplicaciones reutilizables.*

1. La Administración General del Estado mantendrá el Directorio general de aplicaciones para su libre reutilización, de acuerdo al artículo 158 de la Ley 40/2015, de 1 octubre, a través del Centro de Transferencia de Tecnología. Este directorio podrá ser utilizado por otras Administraciones Públicas. En el caso de disponer de un directorio propio, deberá garantizar que las aplicaciones disponibles en ese directorio propio se pueden consultar también a través del Centro de Transferencia de Tecnología.

2. Las Administraciones Públicas conectarán los directorios de aplicaciones para su libre reutilización entre sí; y con instrumentos equivalentes del ámbito de la Unión Europea.

3. Las Administraciones Públicas publicarán las aplicaciones reutilizables, en modo producto o en modo servicio, en los directorios de aplicaciones para su libre reutilización, con al menos el siguiente contenido:

a) Código fuente de las aplicaciones finalizadas, en el caso de ser reutilizables en modo producto y haber sido declaradas de fuentes abiertas.

b) Documentación asociada.

c) Condiciones de licenciamiento de todos los activos, en el caso de ser reutilizables en modo producto, o nivel de servicio ofrecido, en el caso de ser reutilizables en modo servicio.

d) Los costes asociados a su reutilización, en el caso de que existieran.

4. Las Administraciones procurarán la incorporación a la aplicación original de aquellas modificaciones o adaptaciones realizadas sobre cualquier aplicación que se haya obtenido desde un directorio de aplicaciones reutilizables.»

Seis. Se modifica el artículo 18, que queda redactado como sigue:

**«Artículo 18.** *Interoperabilidad en la política de firma electrónica y de certificados.*

1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para el reconocimiento mutuo de las firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Públicas.

Todos los organismos y entidades de derecho público de la Administración General del Estado aplicarán la política de firma electrónica y de certificados a que se refiere el párrafo anterior. La no aplicación de dicha política deberá ser justificada por el órgano u organismo competente y autorizada por la Secretaría General de Administración Digital.

2. Las restantes Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados a que hace referencia el apartado anterior.

3. Sin perjuicio de lo expuesto en el apartado anterior, las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales.

Las políticas de firma electrónica que aprueben las Administraciones Públicas partirán de la norma técnica establecida a tal efecto en la disposición adicional primera, de los estándares técnicos existentes, y deberán ser interoperables con la política marco de firma electrónica mencionada en el apartado 1, en particular, con sus ficheros de implementación. La Administración Pública proponente de una política de firma electrónica particular garantizará su interoperabilidad con la citada política marco de firma electrónica y con sus correspondientes ficheros de implementación según las condiciones establecidas en la norma técnica de interoperabilidad recogida a tal efecto en la disposición adicional primera.

4. Al objeto de garantizar la interoperabilidad de las firmas electrónicas emitidas conforme a las políticas establecidas, las políticas de firma electrónica que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

5. Las Administraciones Públicas receptoras de documentos electrónicos firmados, siempre que hayan admitido con anterioridad la política de firma del emisor, permitirán la validación de las firmas electrónicas según la política de firma indicada en la firma del documento electrónico.

6. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones Públicas sin ningún tipo de restricción técnica, semántica u organizativa.

7. Los procedimientos en los que se utilicen certificados de firma electrónica deberán atenerse a la política de firma electrónica y de certificados aplicable en su ámbito, particularmente en la aplicación de los datos obligatorios y opcionales, las

reglas de creación y validación de firma electrónica, los algoritmos a utilizar y longitudes de clave mínimas aplicables.»

Siete. Se elimina el artículo 19.
Ocho. Se modifica la disposición adicional primera, que queda redactada como sigue:

**«Disposición adicional primera.** *Desarrollo del Esquema Nacional de Interoperabilidad.*

1. Se desarrollarán las siguientes normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones Públicas:

a) Norma Técnica de Catálogo de estándares: establecerá un conjunto de estándares que satisfagan lo previsto en el artículo 11 de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados.

b) Norma Técnica de Documento electrónico: tratará los metadatos mínimos obligatorios, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados; y los formatos de documento.

c) Norma Técnica de Digitalización de documentos: tratará los formatos y estándares aplicables, los niveles de calidad, las condiciones técnicas y los metadatos asociados al proceso de digitalización.

d) Norma Técnica de Expediente electrónico: tratará de su estructura y formato, así como de las especificaciones de los servicios de remisión y puesta a disposición.

e) Norma Técnica de Política de firma electrónica y de certificados de la Administración: Tratará, entre otras cuestiones recogidas en su definición en el anexo, aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones Públicas.

f) Norma Técnica de Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en las Administraciones Públicas y que serán de aplicación para los prestadores y consumidores de tales servicios.

g) Norma Técnica de Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras Administraciones.

h) Norma Técnica de Política de gestión de documentos electrónicos: incluirá directrices para la asignación de responsabilidades, tanto directivas como profesionales, y la definición de los programas, procesos y controles de gestión de documentos y administración de los repositorios electrónicos, y la documentación de los mismos, a desarrollar por las Administraciones Públicas y por los organismos públicos y entidades de derecho público vinculados o dependientes de aquéllas.

i) Norma Técnica de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas.

j) Norma Técnica de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.

k) Norma Técnica de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales: tratará de aspectos funcionales y técnicos para el intercambio de asientos registrales, gestión de errores y excepciones, gestión de anexos, requerimientos tecnológicos y transformaciones de formatos.

l) Norma Técnica de Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de información puestos a disposición del público por medios electrónicos para su reutilización.

m) Norma Técnica de interoperabilidad de inventario y codificación de objetos administrativos: tratará las reglas relativas a la codificación de objetos

administrativos, así como la conexión entre los inventarios correspondientes, incluyendo, por un lado, las unidades orgánicas y oficinas de la Administración, y, por otro lado, la información administrativa de procedimientos y servicios.

n) Norma Técnica de Interoperabilidad de Transferencia e Ingreso de documentos y expedientes electrónicos: tratará los requisitos y condiciones relativos a la transferencia de agrupaciones documentales en formato electrónico, documentos y expedientes electrónicos, junto con los metadatos asociados, entre sistemas de gestión de documentos electrónicos y sistemas de archivo electrónico.

ñ) Norma Técnica de Interoperabilidad de Valoración y Eliminación de documentos y expedientes electrónicos: tratará las condiciones y requisitos relativos a la valoración de los documentos y expedientes electrónicos para establecimiento de plazos de conservación, transferencia y acceso o, en su caso, eliminación total o parcial.

o) Norma Técnica de Interoperabilidad de preservación de documentación electrónica: tratará las condiciones y requisitos relativos a la conservación de los documentos electrónicos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, así como la protección, recuperación y conservación física y lógica de los documentos y su contexto.

p) Norma Técnica de Interoperabilidad de tratamiento y preservación de bases de datos: tratará las condiciones y requisitos relativos a la conservación de las bases de datos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, y permitiendo la protección, recuperación y conservación física y lógica de los datos y su contexto.

q) Norma Técnica de Interoperabilidad de Plan de Direccionamiento: tratará reglas aplicables a la asignación y requisitos de direccionamiento IP para garantizar la correcta administración de la Red de comunicaciones de las Administraciones Públicas españolas y evitar el uso de direcciones duplicadas.

r) Norma Técnica de Interoperabilidad de reutilización de activos en modo producto y en modo servicio: tratará los requisitos y condiciones para facilitar la reutilización de activos tanto en modo producto como en modo servicio por las Administraciones Públicas españolas.

s) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros de funcionarios habilitados: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de funcionarios habilitados pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas.

t) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros electrónicos de apoderamientos: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, A los registros mercantiles, de la propiedad, y a los protocolos notariales.

u) Norma Técnica de Interoperabilidad de Sistema de Referencia de documentos y repositorios de confianza: tratará los requisitos técnicos que deberán cumplir las referencias a documentos al ser intercambiadas, de forma que se evite trasladar documentación de forma innecesaria.

v) Norma Técnica de Política de firma electrónica y de certificados en el ámbito estatal: tratará las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación, organizadas alrededor de los conceptos de generación y validación de firma e incluirá los perfiles interoperables de los medios de identificación de las Administraciones Públicas previstos en Ley 40/2015, de 1 de octubre.

2. El Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica prevista en la disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, aprobará las normas técnicas de interoperabilidad y las publicará mediante Resolución de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

3. Para la redacción y actualización de las normas técnicas de interoperabilidad indicadas en el apartado 1 y las futuras que pueda aprobar el Ministerio de Asuntos Económicos y Transformación Digital que sean necesarias para garantizar el adecuado nivel de interoperabilidad como consecuencia del nivel de desarrollo tecnológico, los compromisos internacionales o el marco normativo aplicable, se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de Administración electrónica.

Para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, el órgano competente será el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia.

4. Se desarrollarán los siguientes instrumentos para la interoperabilidad:

a) Sistema de Información Administrativa: Inventario de procedimientos administrativos, servicios prestados y otras actuaciones administrativas que generen documentación pública, conteniendo información de los mismos clasificada por funciones y con indicación de su nivel de informatización, así como información acerca de las interfaces al objeto de favorecer la interacción o en su caso la integración de los procesos.

b) Centro de interoperabilidad semántica de la Administración: Almacenará, publicará y difundirá los modelos de datos de los servicios de interoperabilidad entre Administraciones Públicas y de estas con los ciudadanos, tanto comunes como sectoriales, así como los relativos a infraestructuras y servicios comunes, además de las especificaciones semánticas y codificaciones relacionadas. Su propósito es facilitar la comprensión semántica de los servicios de intercambio de datos de las Administraciones y maximizar la reutilización de activos semánticos en la construcción de éstos. Se conectará con otros instrumentos equivalentes de las Administraciones Públicas y del ámbito de la Unión Europea.

c) Centro de Transferencia de Tecnología: Directorio de aplicaciones para su libre reutilización que contendrá la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

d) Directorio Común de Unidades Orgánicas y Oficinas de las Administraciones Públicas: Instrumento que permitirá la sincronización de los sistemas que traten la información de inventariado, codificación y evolución de unidades orgánicas y oficinas en diferentes modalidades de integración para garantizar la flexibilidad tanto en el consumo como en la provisión de información relacionada.»

Nueve. Se suprime la disposición adicional tercera.

Diez. Se suprime la disposición adicional cuarta.

Once. Se modifica el anexo de la forma siguiente:

1. Se suprime el término « Familia».

2. A continuación del término «Índice electrónico» se sustituye el vigente término «Infraestructuras y servicios comunes» por el término «Infraestructura o servicio común» con la siguiente redacción:

«Infraestructura o servicio común: capacidad organizativa y técnica que satisface necesidades comunes de los usuarios en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.»

3. A continuación del término «Estándar abierto» se introduce el término «Ficheros de implementación de las políticas de firma« con la siguiente redacción:

«Ficheros de implementación de las políticas de firma: Son la representación en lenguaje formal (XML o ASN.1) de las condiciones establecidas en la política de firma, acorde a las normas técnicas establecidas por los organismos de estandarización.»

**Disposición final tercera.** *Modificación del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo.*

Se modifican el párrafo segundo de la letra d) y la letra g) del apartado 1 del artículo 2 del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo, que quedan redactados como sigue:

«2.º El Impacto presupuestario comprenderá, al menos, una referencia a los efectos en los ingresos y gastos públicos e incluirá la incidencia en los gastos de personal, dotaciones o retribuciones, gastos en medios o servicios de la Administración digital o cualesquiera otros gastos al servicio del sector público.»

«g) Otros impactos: La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma.»

**Disposición final cuarta.** *Habilitación normativa.*

Se faculta a la persona titular del Ministerio de Política Territorial y Función Pública y a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital en el ámbito de sus competencias, para dictar las disposiciones y adoptar las medidas necesarias para el desarrollo y ejecución de este real decreto y del Reglamento que aprueba, así como para modificar el anexo del mismo.

**Disposición final quinta.** *Entrada en vigor.*

Este real decreto entrará en vigor el día 2 de abril de 2021.

## REGLAMENTO DE ACTUACIÓN Y FUNCIONAMIENTO DEL SECTOR PÚBLICO POR MEDIOS ELECTRÓNICOS

### TÍTULO PRELIMINAR

### Disposiciones generales

**Artículo 1.** *Objeto y ámbito de aplicación.*

1. Este Reglamento tiene por objeto el desarrollo de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en lo referido a la actuación y el funcionamiento electrónico del sector público.

2. El ámbito subjetivo de aplicación es el establecido en el artículo 2 de la Ley 39/2015, de 1 de octubre, y el artículo 2 de la Ley 40/2015, de 1 de octubre.

**Artículo 2.** *Principios generales.*

El sector público deberá respetar los siguientes principios en sus actuaciones y relaciones electrónicas:

a) Los principios de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías y sistemas de comunicaciones electrónicas, para garantizar tanto la independencia en la elección de las alternativas tecnológicas necesarias para relacionarse

con las Administraciones Públicas por parte de las personas interesadas y por el propio sector público, como la libertad para desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos, el sector público utilizará estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado.

Las herramientas y dispositivos que deban utilizarse para la comunicación por medios electrónicos, así como sus características técnicas, serán no discriminatorios, estarán disponibles de forma general y serán compatibles con los productos informáticos de uso general.

b) El principio de accesibilidad, entendido como el conjunto de principios y técnicas que se deben respetar al diseñar, construir, mantener y actualizar los servicios electrónicos para garantizar la igualdad y la no discriminación en el acceso de las personas usuarias, en particular de las personas con discapacidad y de las personas mayores.

c) El principio de facilidad de uso, que determina que el diseño de los servicios electrónicos esté centrado en las personas usuarias, de forma que se minimice el grado de conocimiento necesario para el uso del servicio.

d) El principio de interoperabilidad, entendido como la capacidad de los sistemas de información y, por ende, de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos.

e) El principio de proporcionalidad, en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos.

f) El principio de personalización y proactividad, entendido como la capacidad de las Administraciones Públicas para que, partiendo del conocimiento adquirido del usuario final del servicio, proporcione servicios precumplimentados y se anticipe a las posibles necesidades de los mismos.

**Artículo 3.** *Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas.*

1. Estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los sujetos a los que se refiere el artículo 14.2 de la Ley 39/2015, de 1 de octubre.

2. Las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas podrán ejercitar su derecho a relacionarse electrónicamente con la Administración Pública de que se trate al inicio del procedimiento y, a tal efecto, lo comunicarán al órgano competente para la tramitación del mismo de forma que este pueda tener constancia de dicha decisión. La voluntad de relacionarse electrónicamente o, en su caso, de dejar de hacerlo cuando ya se había optado anteriormente por ello, podrá realizarse en una fase posterior del procedimiento, si bien deberá comunicarse a dicho órgano de forma que quede constancia de la misma. En ambos casos, los efectos de la comunicación se producirán a partir del quinto día hábil siguiente a aquel en que el órgano competente para tramitar el procedimiento haya tenido constancia de la misma.

3. De acuerdo con lo previsto en el apartado 3 del artículo 14 de la Ley 39/2015, de 1 de octubre, la obligatoriedad de relacionarse electrónicamente podrá establecerse reglamentariamente por las Administraciones Públicas para determinados procedimientos y para ciertos colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos, quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

A tal efecto, en el ámbito estatal la mencionada obligatoriedad de relacionarse por medios electrónicos con sus órganos, organismos y entidades de derecho público podrá ser establecida por real decreto acordado en Consejo de Ministros o por orden de la persona titular del Departamento competente respecto de los procedimientos de que se trate que afecten al ámbito competencial de uno o varios Ministerios cuya regulación no requiera de norma con rango de real decreto. Asimismo, se publicará en el Punto de Acceso General electrónico (PAGe) de la Administración General del Estado y en la sede electrónica o sede asociada que corresponda.

**Artículo 4.** *Canales de asistencia para el acceso a los servicios electrónicos.*

Las Administraciones Públicas prestarán la asistencia necesaria para facilitar el acceso de las personas interesadas a los servicios electrónicos proporcionados en su ámbito competencial a través de alguno o algunos de los siguientes canales:

a) Presencial, a través de las oficinas de asistencia que se determinen.
b) Portales de internet y sedes electrónicas.
c) Redes sociales.
d) Telefónico.
e) Correo electrónico.
f) Cualquier otro canal que pueda establecerse de acuerdo con lo previsto en el artículo 12 de la Ley 39/2015, de 1 de octubre.

## TÍTULO I

## Portales de internet, Punto de Acceso General electrónico y sedes electrónicas

**Artículo 5.** *Portales de internet de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 39 de la Ley 40/2015, de 1 de octubre, se entiende por portal de internet el punto de acceso electrónico cuya titularidad corresponda a una Administración Pública, organismo público o entidad de derecho público que permite el acceso a través de internet a la información y, en su caso, a la sede electrónica o sede electrónica asociada correspondiente.
2. Cada Administración podrá determinar los contenidos y canales mínimos de atención a las personas interesadas y de difusión y prestación de servicios que deban tener sus portales, así como criterios obligatorios de imagen institucional. En cualquier caso, deberán tenerse en cuenta los contenidos, formatos y funcionalidades que en la normativa de reutilización, accesibilidad y transparencia se establezcan como obligatorios para los sitios web.
3. Los portales de internet dispondrán de sistemas que permitan el establecimiento de medidas de seguridad de acuerdo con lo establecido en Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

**Artículo 6.** *Creación y supresión de portales de internet en el ámbito estatal.*

1. En el ámbito estatal, la creación o supresión de portales se llevará a cabo por orden de la persona titular del ministerio correspondiente o por resolución de la persona titular del órgano superior, en el caso de la Administración General del Estado, y por resolución de la persona titular de la Presidencia o de la Dirección en el caso de sus organismos públicos y entidades de derecho público vinculados o dependientes.

La creación requerirá informe favorable de la Comisión Ministerial de Administración Digital respectiva y posterior comunicación al Ministerio de Política Territorial y Función Pública y al Ministerio de Asuntos Económicos y Transformación Digital. Para obtener dicho informe favorable, la propuesta de creación del nuevo portal se deberá justificar en términos de eficiencia en la asignación y utilización de los recursos públicos e interés prioritario para la implantación de una política pública o la aplicación de la normativa de la Unión Europea o nacional y a tal efecto el órgano promotor de la creación del nuevo portal remitirá una memoria justificativa y económica.

La supresión de portales requerirá la previa comunicación al Ministerio de Política Territorial y Función Pública y al Ministerio de Asuntos Económicos y Transformación Digital.

2. El acto o resolución de creación de un nuevo portal previsto en el apartado anterior contendrá, al menos, la identificación de su dirección electrónica, que deberá incluir el nombre de dominio de segundo nivel «.gob.es», su ámbito funcional y, en su caso, orgánico y la finalidad para la que se crea. Para facilitar su identificación, seguirán las disposiciones generales que se establezcan para la imagen institucional de la Administración General del Estado.

3. En el ámbito estatal los portales de internet a los que se refiere este artículo deberán estar referenciados en el PAGe de la Administración General del Estado.

**Artículo 7.** *Punto de Acceso General electrónico.*

1. Las Administraciones Públicas contarán con un Punto de Acceso General electrónico (PAGe).

2. El PAGe de cada Administración Pública facilitará el acceso a los servicios, trámites e información de los órganos, organismos públicos y entidades vinculados o dependientes de la Administración Pública correspondiente.

3. El PAGe dispondrá de una sede electrónica, a través de la cual se podrá acceder a todas las sedes electrónicas y sedes asociadas de la Administración Pública correspondiente.

Además, esta sede podrá incluir un área personalizada a través de la cual cada interesado, mediante procedimientos seguros que garanticen la integridad y confidencialidad de sus datos personales, podrá acceder a su información, al seguimiento de los trámites administrativos que le afecten y a las notificaciones y comunicaciones en el ámbito de la Administración Pública competente.

4. El PAGe de la Administración General del Estado y su sede electrónica serán gestionados por el Ministerio de Política Territorial y Función Pública en colaboración con la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

En dicha sede electrónica está alojada la Dirección Electrónica Habilitada única a la que se refiere el artículo 43 de la Ley 39/2015, de 1 de octubre.

El PAGe de la Administración General del Estado, a través de su sede, permitirá la comprobación de la autenticidad e integridad de los documentos facilitados por el sector público estatal a través del Código Seguro de Verificación o de cualquier otro sistema de firma o sello basado en certificado electrónico cualificado que se haya utilizado en su generación. También permitirá, en su caso, su recuperación.

5. El PAGe de la Administración General del Estado podrá interoperar con portales web oficiales de la Unión Europea.

**Artículo 8.** *Carpeta Ciudadana del sector público estatal.*

1. La Carpeta Ciudadana es el área personalizada de las personas interesadas a que se refiere el artículo 7.3 en su relación con el sector público estatal. Además del interesado podrán acceder a la Carpeta Ciudadana:

a) Sus representantes legales.

b) Quien ostente un poder general previsto en el artículo 6.4.a) de la Ley 39/2015, de 1 de octubre, otorgado por el interesado e inscrito en el Registro Electrónico de Apoderamientos.

2. La Carpeta Ciudadana será accesible a través de la sede electrónica del PAGe de la Administración General del Estado y podrá ofrecer, entre otras, las funcionalidades siguientes para el interesado o sus representantes:

a) Permitir el seguimiento del estado de tramitación de los procedimientos en que sea interesado, de acuerdo con lo previsto en el artículo 53.1.a) de la Ley 39/ 2015, de 1 de octubre.

b) Permitir el acceso a sus comunicaciones y notificaciones.

c) Conocer qué datos suyos obran en poder del sector público estatal, sin perjuicio de las limitaciones que establezca la normativa vigente.

d) Facilitar la obtención de certificaciones administrativas exigidas por la normativa correspondiente.

3. El interesado accederá a la Carpeta Ciudadana mediante los sistemas de identificación a los que se refiere el artículo 9.2 de la Ley 39/2015, de 1 de octubre.

4. El interesado deberá asegurar el buen uso de los sistemas de identificación y velar por que el acceso a su carpeta Ciudadana solo se haga por sí mismo o por tercero autorizado.

**Artículo 9.** *Sedes electrónicas de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, una sede electrónica es aquella dirección electrónica disponible para la ciudadanía por medio de redes de telecomunicaciones. Mediante dicha sede electrónica se realizarán todas las actuaciones y trámites referidos a procedimientos o a servicios que requieran la identificación de la Administración Pública y, en su caso, la identificación o firma electrónica de las personas interesadas.

2. La titularidad de la sede electrónica corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de derecho público en el ámbito de sus competencias.

**Artículo 10.** *Creación y supresión de las sedes electrónicas y sedes electrónicas asociadas.*

1. Se podrán crear una o varias sedes electrónicas asociadas a una sede electrónica atendiendo a razones técnicas y organizativas. La sede electrónica asociada tendrá consideración de sede electrónica a todos los efectos.

2. El acto o resolución de creación o supresión de una sede electrónica o sede electrónica asociada será publicado en el boletín oficial que corresponda en función de cuál sea la Administración Pública titular de la sede o sede asociada y también en el directorio del Punto de Acceso General Electrónico que corresponda. En el caso de las entidades locales, el boletín oficial será el de la provincia al que pertenezca la entidad.

El acto o resolución de creación determinará, al menos:

a) El ámbito de aplicación de la sede electrónica o sede electrónica asociada.

b) La identificación de la dirección electrónica de referencia de la sede electrónica o sede electrónica asociada que se cree, así como de las direcciones electrónicas de las sedes electrónicas que desde el momento de la creación ya sean asociadas de aquella. Las sedes electrónicas asociadas con posterioridad a la publicación del instrumento de creación se referenciarán en la mencionada dirección electrónica.

c) La identificación de su titular.

d) La identificación del órgano u órganos encargados de la gestión y de los servicios puestos a disposición en la misma.

3. En el ámbito estatal, tanto la creación o supresión de una sede electrónica asociada a la sede electrónica del PAGe de la Administración General del Estado como la creación o supresión de sedes electrónicas o sedes electrónicas asociadas de los organismos públicos y entidades de derecho público vinculados o dependientes se hará mediante orden de la persona titular del Departamento competente o por resolución de la persona titular de la Presidencia o de la Dirección del organismo o entidad de derecho público competente, con el informe previo favorable del Ministerio de Política Territorial y Función Pública y del Ministerio de Asuntos Económicos y Transformación Digital.

4. Para obtener los informes previos favorables a que se refiere el apartado anterior, la propuesta de creación de la nueva sede electrónica o, en su caso, sede electrónica asociada se tendrá que justificar, en términos de eficiencia en la asignación y utilización de recursos públicos. A tal efecto, el órgano promotor de la creación de la sede electrónica remitirá una memoria justificativa y económica en que se explicite el volumen de trámites que está previsto gestionar a través de la misma, los efectos presupuestarios y económicos de su establecimiento, su incidencia en la reducción del tiempo de resolución de los procedimientos y de cargas administrativas para las personas interesadas y cualquier otra razón de interés general que justifique su creación.

**Artículo 11.** *Contenido y servicios de las sedes electrónicas y sedes asociadas.*

1. Toda sede electrónica o sede electrónica asociada dispondrá del siguiente contenido mínimo a disposición de las personas interesadas:

a) La identificación de la sede electrónica o sede electrónica asociada, así como del órgano u organismo titular de la misma y los órganos competentes para la gestión de la información, servicios, procedimientos y trámites puestos a disposición en ella.

b) La identificación del acto o disposición de creación y el acceso al mismo, directamente o mediante enlace a su publicación en el Boletín Oficial correspondiente.

c) La información necesaria para la correcta utilización de la sede electrónica, incluyendo su mapa o información equivalente, con especificación de la estructura de navegación y las distintas secciones disponibles, así como la relativa a propiedad intelectual, protección de datos personales y accesibilidad.

d) La relación de sistemas de identificación y firma electrónica que sean admitidos o utilizados en la misma.

e) La normativa reguladora del Registro al que se acceda a través de la sede electrónica.

f) La fecha y hora oficial, así como el calendario de días inhábiles a efectos del cómputo de plazos aplicable a la Administración en que se integre el órgano, organismo público o entidad de derecho público vinculado o dependiente que sea titular de la sede electrónica o sede electrónica asociada.

g) Información acerca de cualquier incidencia técnica que acontezca e imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, así como de la ampliación del plazo no vencido que, en su caso, haya acordado el órgano competente debido a dicha circunstancia.

h) Relación actualizada de los servicios, procedimientos y trámites disponibles

i) Relación actualizada de las actuaciones administrativas automatizadas vinculadas a los servicios, procedimientos y trámites descritos en la letra anterior. Cada una se acompañará de la descripción de su diseño y funcionamiento, los mecanismos de rendición de cuentas y transparencia, así como los datos utilizados en su configuración y aprendizaje.

2. Las sedes electrónicas y sedes electrónicas asociadas dispondrán, al menos, de los siguientes servicios a disposición de las personas interesadas:

a) Un acceso a los servicios y trámites disponibles en la sede electrónica o sede electrónica asociada, con indicación de los plazos máximos de duración de los procedimientos, excluyendo las posibles ampliaciones o suspensiones que en su caso, pudiera acordar el órgano competente.

b) Un enlace para la formulación de sugerencias y quejas ante los órganos que en cada caso resulten competentes.

c) Los mecanismos de comunicación y procedimiento de reclamación establecidos al respecto de los requisitos de accesibilidad de los sitios web y aplicaciones móviles del sector público.

d) Un sistema de verificación de los certificados de la sede electrónica.

e) Un sistema de verificación de los sellos electrónicos de los órganos, organismos públicos o entidades de derecho público que abarque la sede electrónica o sede electrónica asociada.

f) Un servicio de comprobación de la autenticidad e integridad de los documentos emitidos por los órganos, organismos públicos o entidades de derecho público comprendidos en el ámbito de la sede electrónica, que hayan sido firmados por cualquiera de los sistemas de firma conformes a la Ley 40/2015, 1 de octubre, y para los cuales se haya generado un código seguro de verificación.

g) Un acceso a los modelos, y sistemas de presentación masiva, de uso voluntario, que permitan a las personas interesadas presentar simultáneamente varias solicitudes en la forma que establezca, en su caso, cada Administración, organismo público o entidad de derecho público titular de la sede electrónica o sede electrónica asociada.

h) El acceso a los modelos normalizados de presentación de solicitudes que establezca, en su caso, cada Administración u organismo público o entidad de derecho público titular de la sede electrónica o sede electrónica asociada.

i) Un servicio de consulta del directorio geográfico de oficinas de asistencia en materia de registros, que permita al interesado identificar la más próxima a su dirección de consulta.

3. De acuerdo con lo previsto en el artículo 66.1 de la Ley 39/2015, de 1 de octubre, las Administraciones Públicas deberán mantener y actualizar en la sede electrónica correspondiente un listado con los códigos de identificación vigentes de sus órganos, centros o unidades administrativas.

**Artículo 12.** *Responsabilidad sobre la sede electrónica o sede electrónica asociada.*

1. El titular de la sede electrónica y, en su caso, de la sede electrónica asociada, será responsable de la integridad, veracidad y actualización de la información y los servicios de su competencia a los que pueda accederse a través de la misma.

2. En caso de que la sede electrónica o sede electrónica asociada contenga un enlace o vínculo a otra sede o sede asociada, será el titular de esta última el responsable de la integridad, veracidad y actualización de la información o procedimientos que figuren en la misma, sin perjuicio de la debida diligencia del titular de la primera respecto de la incorporación de los contenidos en la misma.

3. En caso de que una sede electrónica o sede electrónica asociada contenga procedimientos, servicios o ambos, cuya competencia corresponda a otro órgano administrativo, organismo público o entidad de derecho público vinculado o dependiente, sea de la misma o de diferente Administración, el titular de la competencia será responsable de la integridad, veracidad y actualización de lo relativo a dichos procedimientos, servicios o ambos sin perjuicio de la debida diligencia del titular de la sede electrónica o sede electrónica asociada respecto de la incorporación de los contenidos en la misma.

## TÍTULO II

## Procedimiento administrativo por medios electrónicos

### CAPÍTULO I

### Disposiciones generales

**Artículo 13.** *Actuación administrativa automatizada.*

1. La tramitación electrónica de una actuación administrativa podrá llevarse a cabo, entre otras formas, de manera automatizada de acuerdo con lo previsto en el artículo 41 de la Ley 40/2015, de 1 de octubre.

2. En el ámbito estatal la determinación de una actuación administrativa como automatizada se autorizará por resolución del titular del órgano administrativo competente por razón de la materia o del órgano ejecutivo competente del organismo o entidad de derecho público, según corresponda, y se publicará en la sede electrónica o sede electrónica asociada. La resolución expresará los recursos que procedan contra la actuación, el órgano administrativo o judicial, en su caso, ante el que hubieran de presentarse y plazo para interponerlos, sin perjuicio de que las personas interesadas puedan ejercitar cualquier otro que estimen oportuno y establecerá medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos de las personas interesadas.

3. En el ámbito de las Entidades Locales, en caso de actuación administrativa automatizada se estará a lo dispuesto en la disposición adicional octava del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional.

**Artículo 14.** *Régimen de subsanación.*

1. Si existe la obligación del interesado de relacionarse a través de medios electrónicos y aquel no los hubiese utilizado, el órgano administrativo competente en el ámbito de actuación requerirá la correspondiente subsanación, advirtiendo al interesado, o en su caso su representante, que, de no ser atendido el requerimiento en el plazo de diez días, se le tendrá por desistido de su solicitud o se le podrá declarar decaído en su derecho al trámite correspondiente, previa resolución que deberá ser dictada en los términos previstos en el artículo 21 de la Ley 39/2015, de 1 de octubre.

Este régimen de subsanación será asimismo aplicable a las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas que, de acuerdo con lo dispuesto en el artículo 3.2, hayan ejercitado su derecho a relacionarse electrónicamente con la Administración Pública de que se trate.

Cuando se trate de una solicitud de iniciación del interesado, la fecha de la subsanación se considerará a estos efectos como fecha de presentación de la solicitud de acuerdo con el artículo 68.4 de dicha ley.

2. De acuerdo con lo establecido en el artículo 39.1 de este Reglamento, en el caso de que las Administraciones Públicas hayan determinado los formatos y estándares a los que deberán ajustarse los documentos presentados por el interesado, si este incumple dicho requisito se le requerirá para que, en el plazo de diez días, subsane el defecto advertido en los términos establecidos en los artículos 68.1, cuando se trate de una solicitud de iniciación, y 73.2, cuando se trate de otro acto, ambos de la Ley 39/2015, de 1 de octubre, con la indicación de que, si así no lo hiciera y previa resolución que deberá ser dictada en los términos previstos en el artículo 21 de dicha ley, se le tendrá por desistido de su solicitud o se le podrá declarar decaído en su derecho al trámite correspondiente, respectivamente.

3. En el caso de que el escrito o solicitud presentada adolezca de cualquier otro defecto subsanable, por la falta de cumplimiento de los requisitos exigidos en los artículos 66, 67 y 73 de la Ley 39/2015, de 1 de octubre, o por la falta de otros requisitos exigidos por la legislación específica aplicable, se requerirá su subsanación en el plazo de diez días, en los términos de los artículos 68.1 y 73.1 de la citada ley. Este plazo podrá ser ampliado hasta cinco días, a petición del interesado o a iniciativa del órgano, cuando la aportación de los documentos requeridos, en su caso, presente dificultades especiales, siempre que no se trate de procedimientos selectivos o de concurrencia competitiva.

## CAPÍTULO II

## De la identificación y autenticación de las Administraciones Públicas y las personas interesadas

### *Sección 1.ª Disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad*

**Artículo 15.** *Sistemas de identificación, firma y verificación.*

1. Las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la normativa vigente sobre firma electrónica y resulten adecuados para garantizar la identificación de las personas interesadas y, en su caso, la autenticidad e integridad de los documentos electrónicos.

2. Las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para garantizar el origen e integridad de los documentos electrónicos:

a) Sistemas de identificación de las sedes electrónicas y sedes electrónicas asociadas.

b) Sello electrónico basado en un certificado electrónico cualificado y que reúna los requisitos exigidos por la legislación de firma electrónica.

c) Sistemas de firma electrónica para la actuación administrativa automatizada.

d) Firma electrónica del personal al servicio de las Administraciones Públicas.

e) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

3. Las personas interesadas podrán utilizar los siguientes sistemas de identificación y firma en sus relaciones electrónicas con las Administraciones Públicas:

a) De acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas descritos en las letras a), b) y c) de dicho artículo. En este último supuesto los sistemas deberán ser autorizados previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

b) Asimismo, se considerarán válidos a efectos de firma electrónica ante las Administraciones Públicas los sistemas previstos en las letras a), b) y c) del artículo 10.2 de la Ley 39/2015, de 1 de octubre.

c) De acuerdo con lo previsto en el artículo 10.4 de la Ley 39/2015, de 1 de octubre, cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación previstos en dicha ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

4. La Administración no será responsable de la utilización por terceras personas de los medios de identificación personal y firma electrónica del interesado, salvo que concurran los requisitos establecidos en el artículo 32 de la Ley 40/2015, de 1 de octubre, para la exigencia de responsabilidad patrimonial.

**Artículo 16.** *Plataformas de verificación de certificados electrónicos y de otros sistemas de identificación.*

1. La Administración General del Estado dispondrá de una plataforma para la verificación de la vigencia y del contenido de los certificados cualificados admitidos en el sector público. El sistema deberá permitir que tal verificación se pueda llevar a cabo de forma libre y gratuita, para el sector público.

La Secretaría General de Administración Digital será el órgano responsable de esta plataforma, que estará disponible para todo el sector público previa formalización del correspondiente instrumento de adhesión.

2. Esta plataforma dispondrá de una declaración de prácticas de validación en la que se detallarán las obligaciones que se comprometen a cumplir tanto la plataforma como las personas usuarias de la misma en relación con los servicios de verificación. Esta declaración estará disponible al público por vía electrónica y con carácter gratuito.

3. Los prestadores cualificados de servicios de confianza deberán facilitar a esta plataforma el acceso electrónico y gratuito para la verificación de la vigencia de los certificados electrónicos emitidos por aquellos en virtud de su cualificación de acuerdo con la legislación aplicable en materia de servicios electrónicos de confianza.

**Artículo 17.** *Política de firma electrónica y de certificados en el ámbito estatal.*

1. La política de firma electrónica y de certificados en el ámbito estatal, está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica.

2. Sin perjuicio de las obligaciones de los prestadores de servicios de confianza previstas en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y resto de normativa vigente, la política de firma electrónica y certificados deberá contener en todo caso:

a) La definición de su ámbito de aplicación.

b) Los requisitos de las firmas electrónicas presentadas ante los órganos de la Administración General del Estado y de sus organismos públicos y entidades de derecho público vinculados o dependientes.

c) Las especificaciones técnicas y operativas para la definición y prestación de los servicios de confianza asociados a las nuevas formas de identificación y autenticación de la Administración General del Estado y de sus organismos públicos y entidades vinculados o dependientes recogidas en este Reglamento.

3. La política de firma electrónica y certificados en el ámbito estatal será aprobada por Resolución de la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial y se publicará en el «Boletín Oficial del Estado» y en la sede electrónica del PAGe de la Administración General del Estado.

### *Sección 2.ª Identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia*

**Artículo 18.** *Identificación de las sedes electrónicas y de las sedes electrónicas asociadas.*

1. De acuerdo con lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, las sedes electrónicas y sedes electrónicas asociadas utilizarán, para identificarse y garantizar

una comunicación segura con las mismas, certificados cualificados de autenticación de sitio web o medio equivalente. Dichos certificados electrónicos se ajustarán a lo señalado en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad, y la normativa vigente en materia de identidad y firma electrónica.

2. En el ámbito estatal las sedes electrónicas y sedes electrónicas asociadas se identificarán mediante certificados cualificados de autenticación de sitio web.

Con carácter adicional y para su identificación inmediata, los ciudadanos y ciudadanas dispondrán de la información general obligatoria que debe constar en las mismas de acuerdo con lo establecido en este Reglamento. Las direcciones electrónicas que tengan la condición de sede electrónica o sede electrónica asociada deberán hacerlo constar de forma visible e inequívoca. Para facilitar su identificación, seguirán las disposiciones generales que se establezcan para la imagen institucional de la Administración General del Estado y su dirección electrónica incluirá el nombre de dominio «.gob.es».

**Artículo 19.** *Identificación mediante sello electrónico basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.*

1. De acuerdo con lo previsto en el artículo 40 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. Estos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos.

2. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos, publicándose en la sede electrónica o sede asociada o en el portal de internet correspondiente. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

3. En el ámbito estatal, la creación de sellos electrónicos se realizará mediante resolución de la persona titular de la Subsecretaría del Ministerio o de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente, que se publicará en la sede electrónica o sede electrónica asociada correspondiente. En dicha resolución deberá constar:

a) El órgano, organismo público o entidad de derecho público vinculado o dependiente titular del sello, que será el responsable de su utilización, con indicación de su Ministerio de adscripción, vinculación o dependencia.
b) Características técnicas generales del sistema de firma y certificado aplicable.
c) Servicio de validación para la verificación del certificado.
d) Actuaciones y procedimientos en los que podrá ser utilizado.

4. Los certificados de sello electrónico en el ámbito estatal tendrán, al menos, los siguientes contenidos:

a) Descripción del tipo de certificado, con la denominación «sello electrónico».
b) Nombre del suscriptor.
c) Número de identificación fiscal del suscriptor.

**Artículo 20.** *Sistemas de firma electrónica para la actuación administrativa automatizada.*

1. De acuerdo con lo previsto en el artículo 42 de la Ley 40/2015, de 1 de octubre, en la tramitación administrativa automatizada de los procedimientos, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, a que se refiere el artículo 19 de este Reglamento, basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.
b) Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos,

permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

2. Cada Administración determinará los medios admitidos para la firma electrónica en las entidades de derecho privado vinculadas o dependientes cuando estas tramiten procedimientos de forma automatizada en el ejercicio de potestades administrativas.

**Artículo 21.** *Sistemas de firma basados en código seguro de verificación para la actuación administrativa automatizada.*

1. De acuerdo con lo previsto en el artículo 42.b) de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas podrán utilizar sistemas de código seguro de verificación de documentos en el desarrollo de actuaciones automatizadas.

Dicho código vinculará al órgano, organismo público o entidad de derecho público y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento en la sede electrónica o sede electrónica asociada correspondiente mediante un procedimiento de verificación directo y gratuito para las personas interesadas.

2. El sistema de código seguro de verificación deberá garantizar, en todo caso:

a) El origen e integridad de los documentos mediante el acceso a la sede electrónica o sede electrónica asociada correspondiente.

b) El carácter único del código generado para cada documento.

c) Su vinculación con el documento generado y, en su caso, con el firmante. El código seguro de verificación y la dirección electrónica de acceso a la sede electrónica o sede electrónica asociada deberán integrarse preferentemente en todas las páginas del documento firmado con dicho código. Cualquier modificación del documento generado dará lugar a un nuevo documento con un código seguro de verificación diferente.

d) La posibilidad de verificar el documento en la sede electrónica o sede electrónica asociada, como mínimo, por el tiempo que se establezca en la resolución que autorice la utilización de este procedimiento. Una vez que el documento deje de estar disponible en la sede electrónica o sede electrónica asociada, su disponibilidad por otros cauces se regirá por lo dispuesto en la estrategia de conservación implantada por cada Administración Pública a través de su política de gestión documental.

e) Un acceso restringido al documento a quien disponga del código seguro de verificación, sin perjuicio de las garantías adicionales que se puedan establecer.

3. En las comunicaciones de documentos electrónicos a otros órganos, organismos o entidades y cuando así lo determinen las partes implicadas, la interoperabilidad se garantizará mediante la superposición al código seguro de verificación de un sello electrónico de los previstos en el artículo 42 de la Ley 40/2015, de 1 de octubre, como mecanismo de verificación automática del origen e integridad de los documentos electrónicos en los términos que establezca la Norma Técnica de Interoperabilidad de Documento Electrónico.

4. En el ámbito estatal, la utilización de este sistema requerirá resolución de la persona titular de la Subsecretaría del Ministerio o de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente, previo informe del Centro Criptológico Nacional y de la Secretaría General de Administración Digital.

La orden o resolución de creación deberá incluir:

a) Actuaciones a las que es de aplicación el sistema.

b) Órganos responsables de la aplicación del sistema.

c) Disposiciones que resultan de aplicación a la actuación.

d) Sede electrónica o sede electrónica asociada a la que pueden acceder las personas interesadas para la verificación del contenido de la actuación o documento.

e) Plazo de disponibilidad para la verificación en la sede electrónica o sede electrónica asociada del código seguro de verificación aplicado a un documento. Este plazo será al menos de cinco años, salvo que en la normativa especial por razón de la materia se prevea un plazo superior. Transcurrido este tiempo, será necesario solicitarlo al órgano de la

Administración Pública, organismo público o entidad de derecho público que emitió el documento. En este caso, cuando utilice medios electrónicos, la certificación de la verificación se realizará mediante firma electrónica del titular del órgano competente o del empleado o empleada público que tenga atribuida la actuación por aquel órgano.

**Artículo 22.** *Sistemas de firma electrónica del personal al servicio de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 43 de la Ley 40/2015, de 1 de octubre, sin perjuicio de lo previsto en los artículos 18, 19 y 20 de este Reglamento, la actuación de una Administración Pública, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano competente o del empleado o empleada público a través del que se ejerza la competencia.

2. Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal. Estos sistemas podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios.

3. Los certificados electrónicos de empleado público serán cualificados y se ajustarán a lo señalado en el Esquema Nacional de Interoperabilidad y la legislación vigente en materia de identidad y firma electrónica.

4. Cada Administración determinará los medios admitidos para la firma electrónica en las entidades de derecho privado vinculadas o dependientes de esta cuando tramiten procedimientos en el ejercicio de potestades administrativas.

**Artículo 23.** *Certificados electrónicos de empleado público con número de identificación profesional.*

1. Sin perjuicio de lo previsto en el artículo 22.3 de este Reglamento, de acuerdo con lo previsto en el artículo 43.2 de la Ley 40/2015, de 1 de octubre, los prestadores cualificados de servicios de confianza podrán consignar un número de identificación profesional en el certificado electrónico de empleado público, a petición de la Administración en la que presta servicios el empleado o empleada de que se trate, si dicho certificado se va a utilizar en actuaciones que afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones para cuya realización esté legalmente justificado el anonimato. Estos certificados se denominarán «certificados electrónicos de empleado público con número de identificación profesional».

2. En el ámbito estatal corresponderá solicitar la consignación de un número de identificación profesional del empleado o empleada público a la persona titular de la Subsecretaría del ministerio o a la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público en el que preste servicios el empleado o empleada público.

3. La Administración solicitante del certificado conservará la documentación acreditativa de la identidad del titular.

4. Los certificados electrónicos de empleado público con número de identificación profesional serán cualificados y se ajustarán a lo previsto en el Esquema Nacional de Interoperabilidad y la legislación vigente en materia de identidad y firma electrónica y tendrán idéntico uso, capacidad y funcionalidad que el certificado electrónico de empleado público, aunque limitados a las actuaciones que justificaron su emisión.

5. Las autoridades públicas competentes y los órganos judiciales, en el ejercicio de sus funciones y de acuerdo con la normativa vigente, podrán solicitar la revelación de la identidad del titular de un certificado de empleado público con número de identificación profesional mediante petición oficial dirigida a la Administración responsable de su custodia.

**Artículo 24.** *Sistemas de identificación y firma electrónica del personal al servicio de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.*

1. El personal al servicio de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, podrá identificarse con aquellos sistemas que, entre los previstos en la Ley 39/2015, de 1 de octubre, se

establezcan en función del nivel de seguridad que corresponda al trámite de que se trate de acuerdo al Esquema Nacional de Seguridad.

2. Dicho personal podrá firmar mediante sistemas de firma electrónica basados en certificados electrónicos cualificados facilitados específicamente a sus empleados y empleadas. Estos sistemas podrán ser utilizados por estos en el desempeño efectivo de su puesto de trabajo, para los trámites y actuaciones que realicen por razón del mismo, o para relacionarse con las Administraciones públicas cuando estas lo admitan.

3. Se podrá disponer de sistemas de identificación de personal basados en repositorios de empleados públicos que permitan la relación de los empleados y empleadas públicos con servicios y aplicaciones necesarios para el ejercicio de sus funciones que en todo caso garanticen lo previsto en el Esquema Nacional de Seguridad.

4. Los registros de personal de la Administración General del Estado podrán recoger los datos para la identificación electrónica de los empleados y empleadas públicos, así como su cesión a sistemas de identificación de personal basados en repositorios de identidades de empleados públicos.

**Artículo 25.** *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. De acuerdo con lo previsto en el artículo 44 de la Ley 40/2015, de 1 de octubre, los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos, organismos públicos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en este artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a una misma Administración Pública, esta establecerá las condiciones y garantías por las que se regirá, que comprenderán, al menos, la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas Administraciones Públicas, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio suscrito entre aquellas.

4. En el ámbito estatal, las condiciones y garantías a que se refiere el apartado 2 serán establecidas por la Secretaría General de Administración Digital.

5. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan conforme a los requisitos establecidos en el Esquema Nacional de Seguridad

***Sección 3.ª Identificación y firma de las personas interesadas***

**Artículo 26.** *Sistemas de identificación de las personas interesadas en el procedimiento.*

1. De acuerdo con lo previsto en la Ley 39/2015, de 1 de octubre, los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad.

2. En particular, de acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, serán admitidos los siguientes sistemas de identificación electrónica:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

c) Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c).

**Artículo 27.** *Atributos mínimos de los certificados electrónicos cuando se utilizan para la identificación de las personas interesadas ante las Administraciones Públicas.*

1. Los sistemas basados en certificados cualificados de firma electrónica admitidos por las Administraciones Públicas para la identificación electrónica de persona física a que se refiere el artículo 9.2.a) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener como atributos, al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal que conste como tal de manera inequívoca. La comprobación de la identidad y otras circunstancias de los solicitantes del certificado, se realizará de conformidad con lo previsto en el artículo 7 de la Ley 6/2020, de 11 de noviembre.

2. Los certificados electrónicos cualificados de representante de persona jurídica deberán contener, como mínimo, la denominación y el Número de Identificación Fiscal de la persona jurídica y el nombre y apellidos y número de Documento Nacional de Identidad, o Número de Identificación de Extranjero o Número de Identificación Fiscal de la persona que actúa como representante.

3. Los sistemas basados en certificados cualificados de sello electrónico admitidos por las Administraciones Públicas para la identificación electrónica de persona jurídica a que se refiere el artículo 9.2.b) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener, como mínimo, su denominación y su Número de Identificación Fiscal.

**Artículo 28.** *Sistemas de clave concertada y otros sistemas de identificación de las personas interesadas.*

1. Los sistemas de clave concertada o cualquier otro sistema que las Administraciones Públicas consideren válidos, admitidos para la identificación electrónica de persona física de conformidad con el artículo 9.2.c) de la Ley 39/2015, de 1 de octubre, deberán ajustarse a lo previsto en el Esquema Nacional de Seguridad y contener, como mínimo, el nombre y apellidos y el número de Documento Nacional de Identidad, Número de Identificación de Extranjero, Número de Identificación Fiscal y, para los casos en que así se establezca en la definición del sistema, el número de pasaporte.

2. Los sistemas de identificación a que se refiere el apartado anterior deberán ser autorizados previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

3. En el ámbito estatal, la creación de los nuevos sistemas de identificación será aprobada por orden de la persona titular del Ministerio o, en su caso, resolución de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente por razón del ámbito material en que se vaya a utilizar, previa autorización de la Secretaría General de Administración Digital a que se refiere el apartado anterior.

Cuando el nuevo sistema se refiera a la totalidad de la Administración General del Estado se requerirá Acuerdo del Consejo de Ministros a propuesta de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital. En este caso, este sistema deberá estar accesible a través de la Plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.

**Artículo 29.** *Sistemas de firma electrónica de las personas interesadas admitidos por las Administraciones Públicas y régimen de uso.*

1. De acuerdo con lo previsto en el artículo 10.2 de la Ley 39/2015, de 1 de octubre, en el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

c) Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezca, siempre que cuente con un registro previo como usuario que permita garantizar su identidad.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c).

2. El uso de la firma electrónica no excluye la obligación de incluir en el documento o comunicación electrónica los datos de identificación del interesado y, en su caso, del representante o la representante, que sean necesarios de acuerdo con la legislación que le sea aplicable.

3. Los sistemas de firma electrónica que usen las personas interesadas permitirán que las Administraciones Públicas puedan verificar los datos consignados de la firma, de manera que se pueda vincular su identidad con el acto de firma.

4. Los sistemas de firma electrónica previstos en la letra c) del apartado 1 deberán contar con la previa autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. Asimismo, deberán cumplir con lo previsto en el Real Decreto 3/2010, de 8 de enero.

5. De acuerdo con lo previsto en el artículo 10.4 de la Ley 39/2015, de 1 de octubre, cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación previstos en dicha ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de las personas interesadas.

**Artículo 30.** *Identificación o firma electrónica de las personas interesadas mediante personal funcionario público habilitado.*

1. De acuerdo con lo previsto en el segundo párrafo del artículo 12.2 de la Ley 39/2015 de 1 de octubre, si algún interesado no incluido en los apartados 2 y 3 del artículo 14 de la ley no dispusiera de los medios electrónicos necesarios para su identificación o firma electrónica en el procedimiento administrativo, estas podrán ser válidamente realizadas por personal funcionario público habilitado mediante el uso del sistema de firma electrónica del que esté dotado para ello. En este caso, será necesario que el interesado se identifique ante el funcionario o funcionaria y preste su consentimiento expreso para esta actuación, de lo que deberá quedar constancia por escrito para los casos de discrepancia o litigio.

El funcionario habilitado entregará al interesado toda la documentación acreditativa del trámite realizado, así como una copia del documento de consentimiento expreso cumplimentado y firmado, cuyo formulario estará disponible en el Punto de Acceso General Electrónico de la respectiva Administración

2. En el ámbito estatal la identificación y firma electrónica del interesado conforme al procedimiento descrito en el apartado anterior se realizará necesariamente por un funcionario público inscrito a tal efecto en el Registro de Funcionarios Habilitados de la Administración General del Estado.

La identificación o firma electrónica en el procedimiento por personal funcionario público habilitado sólo será válida para los trámites y actuaciones que haya determinado con carácter previo cada ministerio, organismo público o entidad de derecho público vinculado o dependiente y en los términos que se especifiquen mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital. En el PAGe de la Administración General del Estado y en las sedes electrónicas asociadas de cada ministerio o en la sede electrónica o sede asociada del organismo público o entidad de derecho público en su ámbito de competencia, se mantendrá una relación pública, permanentemente actualizada, de dichos trámites y actuaciones.

**Artículo 31.** *Registro de Funcionarios Habilitados de la Administración General del Estado.*

1. Se crea el Registro de Funcionarios Habilitados en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, en el que constarán inscritos:

a) El personal funcionario habilitado para la identificación y firma electrónica de las personas interesadas en aquellos trámites y procedimientos que se determinen por el ministerio, organismo o entidad competente para su tramitación.

b) El personal funcionario habilitado para la expedición de copias auténticas. Esta habilitación será conferida por los órganos a los que corresponda la emisión de los documentos originales, su custodia, el archivo de documentos o que en sus normas de competencia así se haya previsto.

c) El personal funcionario habilitado que presta servicio en las oficinas de asistencia en materia de registros de la Administración General del Estado, que estará habilitados para la identificación y firma electrónica de las personas interesadas en aquellos trámites y procedimientos que se determinen y para la expedición de copias auténticas electrónicas de cualquier documento que estas presenten para que se remita desde la Oficina a la unidad competente para su incorporación a un expediente administrativo.

2. El Registro de Funcionarios Habilitados será gestionado por la Secretaría de Estado de Política Territorial y Función Pública del Ministerio de Política Territorial y Función Pública, en colaboración con la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Este Registro será interoperable con los sistemas equivalentes que ya existan en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.

3. Este Registro deberá ser plenamente interoperable con los registros u otros sistemas equivalentes que se creen por las comunidades autónomas y las entidades locales a los efectos de comprobar la validez de las citadas habilitaciones.

4. Mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se regulará el funcionamiento del Registro de Funcionarios Habilitados

### *Sección 4.ª Acreditación de la representación de las personas interesadas*

**Artículo 32.** *Acreditación en la actuación por medio de representante.*

1. De acuerdo con lo previsto en el artículo 5 de la Ley 39/2015, de 1 de octubre, las personas interesadas con capacidad de obrar podrán actuar ante las Administraciones Públicas por medio de representante, bien sea una persona física con capacidad de obrar bien sea una persona jurídica cuando así esté previsto en sus Estatutos.

2. Los representantes de las personas interesadas obligadas a relacionarse electrónicamente con las Administraciones Públicas están obligados a relacionarse electrónicamente en el ejercicio de dicha representación, de acuerdo con el artículo 14.2 de la Ley 39/2015, de 1 de octubre.

3. La representación puede acreditarse mediante cualquier medio válido en Derecho que deje constancia fidedigna de su existencia, entre otros:

a) Mediante apoderamiento apud acta efectuado por comparecencia personal en las oficinas de asistencia en materia de registros o comparecencia electrónica en la correspondiente sede electrónica o sede electrónica asociada.

b) Mediante acreditación de su inscripción en el registro electrónico de apoderamientos de la Administración Pública competente o en sus registros particulares de apoderamientos.

c) Mediante un certificado electrónico cualificado de representante.

d) Mediante documento público cuya matriz conste en un archivo notarial o de una inscripción practicada en un registro mercantil.

4. En el caso de actuaciones en nombre de persona jurídica, la capacidad de representación podrá acreditarse también mediante certificado electrónico cualificado de representante, entendiéndose en tal caso que el poder de representación abarca cualquier actuación ante cualquier Administración Pública.

5. Asimismo, de acuerdo con lo previsto en el artículo 5.7 de la Ley 39/2015, de 1 de octubre, las Administraciones Públicas podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones por medios electrónicos en representación de las personas interesadas. En la sede electrónica o sede electrónica asociada de cada una de las Administraciones Públicas se publicarán los trámites electrónicos que podrán realizarse con esta representación.

**Artículo 33.** *Registro Electrónico de Apoderamientos de la Administración General del Estado.*

1. A los efectos previstos en el artículo anterior y de acuerdo con el artículo 6 de la Ley 39/2015, de 1 de octubre, en el Registro Electrónico de Apoderamientos de la Administración General del Estado se inscribirán los apoderamientos de carácter general previstos en el artículo 6.4.a) de dicha ley otorgados «apud acta» a favor de representante, presencial o electrónicamente, por quien ostente la condición de interesado en un procedimiento administrativo para actuar en su nombre ante las Administraciones Públicas.

Asimismo, podrán inscribirse los poderes previstos en el artículo 6.4.b) de la ley para actuar ante la Administración General del Estado o ante un organismo público o entidad de Derecho Público vinculado o dependiente de la misma que no cuente con un registro electrónico de apoderamientos particular. Por último, podrán inscribirse los poderes previstos en el artículo 6.4.c) de la ley otorgados para realizar determinados trámites y actuaciones especificados en el poder ante los órganos de la Administración General del Estado o ante un organismo público o entidad de derecho público vinculado o dependiente de dicha Administración que no cuente con el citado registro particular.

Constará en el Registro el bastanteo del poder realizado por los servicios jurídicos correspondientes, sin perjuicio de la apreciación concreta de su suficiencia en la actuación, trámite o procedimiento en que se emplee.

2. El Registro Electrónico de Apoderamientos de la Administración General del Estado será gestionado por el Ministerio de Política Territorial y Función Pública con la colaboración del Ministerio de Asuntos Económicos y Transformación Digital, y será accesible desde la sede electrónica del PAGe de la Administración General del Estado así como desde las sedes y sedes electrónicas asociadas de la Administración General del Estado y de los organismos públicos o entidades de derecho público vinculados o dependientes.

3. Sin perjuicio de este registro general de apoderamientos, cada organismo público o entidad de derecho público vinculado o dependiente de la Administración General del Estado podrá disponer de un registro particular de apoderamientos en el que se inscriban los poderes otorgados por quien ostente la condición de interesado para realizar los trámites específicos de su competencia y cuya gestión corresponderá al propio organismo o entidad.

En estos registros particulares no podrán inscribirse los poderes previstos en el artículo 6.4.a) de la Ley 39/2015, de 1 de octubre.

4. El Registro Electrónico de Apoderamientos y los registros particulares deberán ser interoperables y no tienen carácter público, por lo que el interesado sólo podrá acceder a la información de los apoderamientos de los que sea poderdante o apoderado.

5. Mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y

Transformación Digital se regularán los requisitos y condiciones de funcionamiento del Registro Electrónico de Apoderamientos de la Administración General del Estado.

**Artículo 34.** *Acreditación de la representación mediante certificado electrónico cualificado de representante.*

1. La representación podrá acreditarse ante la Administración con un certificado electrónico cualificado de representante de persona jurídica que sea acorde a lo previsto en el artículo 28 y el Anexo I del al Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, Reglamento eIDAS) y a la Política marco de Firma Electrónica y de certificados a que hace referencia el Esquema Nacional de Interoperabilidad y, además, haya sido expedido a quien tenga un poder general para llevar a cabo cualquier actuación administrativa y ante cualquier Administración.

2. La aceptación de certificados electrónicos cualificados de representante de persona jurídica de alcance no general estará sujeta al Reglamento eIDAS, a la Política Marco de Firma Electrónica y de Certificados a que hace referencia el Esquema Nacional de Interoperabilidad y además, a los requisitos que disponga cada Administración.

**Artículo 35.** *Acreditación y verificación de las representaciones que resulten de un documento público notarial o certificación de un Registro Mercantil.*

1. Cuando la representación alegada resulte de un documento público notarial, o de una certificación expedida por un registro mercantil, el interesado deberá aportar la certificación registral electrónica correspondiente o al menos expresar el código seguro u otro sistema de acceso y verificación del documento electrónico.

2. Las Administraciones Públicas efectuarán la verificación de la autenticidad e integridad del traslado a papel y el acceso a los metadatos necesarios para la tramitación automatizada de la certificación registral electrónica, mediante el acceso electrónico y gratuito a la dirección electrónica que el Consejo General del Notariado o el Colegio de Registradores, respectivamente, habrán de tener habilitada a tales efectos.

3. Asimismo, las Administraciones Públicas, cuando necesiten comprobar la vigencia, revocación o cese de representaciones inscritas en el Registro Mercantil, consultarán electrónicamente y de modo gratuito el Registro Mercantil.

**Artículo 36.** *Autorización de representantes de terceros por la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.*

1. La Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, de acuerdo con lo previsto en el artículo 5.7 de la Ley 39/2015, de 1 de octubre, podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de las personas interesadas.

2. La habilitación requerirá la firma previa de un convenio entre el Ministerio, organismo público o entidad de derecho público vinculado o dependiente competente y la organización o corporación de que se trate, de acuerdo de lo previsto en el capítulo VI del título Preliminar de la Ley 40/2015, de 1 de octubre. El convenio deberá especificar, al menos, los procedimientos y trámites objeto de la habilitación, y las condiciones y obligaciones aplicables tanto a la entidad firmante del convenio, como a las personas físicas o jurídicas habilitadas y determinará la presunción de validez de la representación.

A estos efectos, podrá acordarse un modelo normalizado de convenio que permita dar soporte a esta habilitación en los términos y condiciones que las partes acuerden, conforme a lo dispuesto en la Ley 40/2015, de 1 de octubre, y que incluya como anexo el modelo individualizado de adhesión al convenio que, previendo expresamente la aceptación de su contenido íntegro, deben suscribir las personas físicas o jurídicas miembros de las organizaciones o corporaciones firmantes que se adhieran al mismo.

3. De acuerdo con lo previsto en el artículo 32.5, en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, los trámites electrónicos que podrán realizarse con esta representación se publicarán en la sede electrónica del PAGe de la Administración General del Estado y en las respectivas sedes electrónicas o sedes electrónicas asociadas.

## CAPÍTULO III

## Registros, comunicaciones y notificaciones electrónicas

### *Sección 1.ª Registros electrónicos*

**Artículo 37.** *Registro electrónico.*

1. Las Administraciones Públicas dispondrán de registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones, que deberán ser plenamente interoperables de manera que se garantice su compatibilidad informática e interconexión en los términos previstos en el artículo 16 de la Ley 39/2015, de 1 de octubre y en el artículo 60 de este Reglamento.

2. Cada Administración dispondrá de un Registro Electrónico General en el que hará el asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, organismo público o entidad de derecho público vinculado o dependiente. Los organismos públicos y entidades de derecho público vinculados o dependientes de cada Administración podrán disponer de su propio registro electrónico plenamente interoperable e interconectado con el Registro Electrónico General de la Administración a la que estén vinculados o de la que dependan.

3. Los registros electrónicos admitirán:

a) Documentos electrónicos normalizados correspondientes a los servicios, procedimientos y trámites que se especifiquen conforme a lo dispuesto en la norma de creación del registro, cumplimentados de acuerdo con formatos preestablecidos.

b) Cualquier solicitud, escrito o comunicación distinta de los mencionados en el párrafo anterior dirigido a cualquier Administración Pública.

4. De acuerdo con el artículo 16.8 de la Ley 39/2015, de 1 de octubre, no se tendrán por presentados en el registro aquellos documentos e información cuyo régimen especial establezca otra forma de presentación. En estos supuestos, el órgano administrativo competente para la tramitación del procedimiento comunicará esta circunstancia al interesado e informará de los requisitos exigidos por la legislación específica aplicable

**Artículo 38.** *Registro Electrónico General de la Administración General del Estado.*

1. El Registro Electrónico General de la Administración General del Estado será gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital y se configura como el conjunto agregado de:

a) Los asientos practicados a través de las aplicaciones de que dispongan las unidades que realicen anotaciones en registro.

b) Las anotaciones que se realicen en cualquier aplicación que proporcione soporte a procedimientos específicos.

c) Las anotaciones que se practiquen por medio del servicio electrónico para la presentación de solicitudes, escritos y comunicaciones que no dispongan de modelos normalizados de presentación, independientemente de las Administraciones Públicas u organismos públicos o entidades de derecho público vinculados o dependientes a las que vayan dirigidos. Dicho servicio electrónico será accesible desde la sede electrónica del PAGe de la Administración General del Estado.

2. Las anotaciones en el Registro General de la Administración General del Estado tendrán plena eficacia y validez para todas las Administraciones Públicas.

**Artículo 39.** *Presentación y tratamiento de documentos en registro.*

1. Las Administraciones Públicas podrán determinar los formatos y estándares a los que deberán ajustarse los documentos presentados por las personas interesadas en el registro siempre que cumplan con lo previsto en el Esquema Nacional de Interoperabilidad y normativa correspondiente.

2. En el caso de que se detecte código malicioso susceptible de afectar a la integridad o seguridad del sistema en documentos que ya hayan sido registrados, se requerirá su subsanación al interesado que los haya aportado de acuerdo con lo previsto en el artículo 14.3 de este Reglamento.

3. Los documentos en soporte no electrónico se presentarán a través de las oficinas de asistencia en materia de registros. Cuando se presenten documentos originales o copias auténticas en soporte no electrónico, desde el momento en que sean digitalizados conforme a lo dispuesto en las correspondientes normas técnicas de interoperabilidad, tendrán la consideración de copia electrónica auténtica de documento en soporte papel con la misma validez para su tramitación que los documentos aportados en soporte papel, conforme a las previsiones del artículo 27 de la Ley 39/2015, de 1 de octubre.

4. Cuando el tamaño de los documentos registrados exceda la capacidad que se determine para el Sistema de Interconexión de Registros (SIR), su remisión a la Administración y órgano al que van dirigidos podrá sustituirse por la puesta a disposición de los documentos, previamente depositados en un repositorio de intercambio de ficheros.

En ámbito de la Administración General del Estado dicho repositorio de intercambio de ficheros será de titularidad pública y tanto los documentos depositados como los datos que estos contengan no podrán ser utilizados para fines distintos a los previstos en la normativa que regule el procedimiento para el que han sido objeto de registro.

5. Los documentos presentados en las oficinas de asistencia en materia de registro serán devueltos a las personas interesadas inmediatamente tras su digitalización o, en caso contrario, se les aplicará lo previsto en el artículo 53 de este Reglamento.

6. El archivo de los documentos intercambiados por registro corresponderá al órgano competente para la tramitación del procedimiento, de acuerdo al plazo que determine su normativa.

**Artículo 40.** *Oficinas de asistencia en materia de registros en el ámbito de la Administración General del Estado.*

1. Las Oficinas de asistencia en materia de registros tienen naturaleza de órgano administrativo de acuerdo con lo dispuesto en el artículo 5 de la Ley 40/2015, de 1 de octubre.

La creación de nuevas Oficinas, así como la modificación o supresión de las existentes se realizará conforme a lo previsto en el artículo 59.2 de la Ley 40/2015, de 1 de octubre.

2. La Administración General del Estado contará con un directorio geográfico de las Oficinas de asistencia en materia de registros que será gestionado por el Ministerio de Política Territorial y Función Pública. A tal efecto, el órgano del que dependa la correspondiente Oficina de asistencia deberá comunicar de forma inmediata al citado Ministerio la aprobación de la norma por la que se cree, modifique o suprima dicha oficina, de acuerdo con lo establecido en el Esquema Nacional de Interoperabilidad, garantizando su actualización permanente.

3. Las Oficinas de asistencia en materia de registros desarrollarán las siguientes funciones:

a) La digitalización de las solicitudes, escritos y comunicaciones en papel que se presenten o sean recibidos en la Oficina y se dirijan a cualquier órgano, organismo público o entidad de derecho público de cualquier Administración Pública, así como su anotación en el Registro Electrónico General o Registro electrónico de cada organismo o entidad según corresponda.

b) La anotación, en su caso, de los asientos de salida que se realicen de acuerdo con lo dispuesto en el artículo 16 de la Ley 39/2015, de 1 de octubre.

c) La emisión del correspondiente recibo que acredite la fecha y hora de presentación de solicitudes, comunicaciones y documentos que presenten las personas interesadas.

d) La expedición de copias electrónicas auténticas tras la digitalización de cualquier documento original o copia auténtica que presenten las personas interesadas y que se vaya a incorporar a un expediente administrativo a través de dicha oficina en el registro electrónico correspondiente.

e) La información en materia de identificación y firma electrónica, para la presentación de solicitudes, escritos y comunicaciones a través de medios electrónicos en los trámites y procedimientos para los que se haya conferido habilitación.

f) La identificación o firma electrónica del interesado, cuando se trate de una persona no obligada a la relación electrónica con la Administración, en los procedimientos administrativos para los que se haya previsto habilitación.

g) La práctica de notificaciones, en el ámbito de actuación de esa Oficina, cuando el interesado o su representante comparezcan de forma espontánea en la Oficina y solicite la comunicación o notificación personal en ese momento.

h) La comunicación a las personas interesadas del código de identificación del órgano, organismo público o entidad a la que se dirige la solicitud, escrito o comunicación.

i) La iniciación de la tramitación del apoderamiento presencial apud acta en los términos previstos en el artículo 6 de la Ley 39/2015, de 1 de octubre.

j) Cualesquiera otras funciones que se les atribuyan legal o reglamentariamente.

### *Sección 2.ª Comunicaciones y notificaciones electrónicas*

**Artículo 41.** *Comunicaciones administrativas a las personas interesadas por medios electrónicos.*

Cuando de acuerdo con lo previsto en el artículo 14 de la Ley 39/2015, de 1 de octubre, la relación de las personas interesadas con las Administraciones Públicas deba realizarse por medios electrónicos, serán objeto de comunicación al interesado por medios electrónicos, al menos:

a) La fecha y, en su caso, hora efectiva de inicio del cómputo de plazos que haya de cumplir la Administración tras la presentación del documento o documentos en el registro electrónico, de acuerdo con lo previsto en el artículo 31.2.c) de la Ley 39/2015, de 1 de octubre.

b) La fecha en que la solicitud ha sido recibida en el órgano competente, el plazo máximo para resolver el procedimiento y para la práctica de la notificación de los actos que le pongan término, así como de los efectos del silencio administrativo, de acuerdo con lo previsto en el artículo 21.4 de la Ley 39/2015, de 1 de octubre.

c) La solicitud de pronunciamiento previo y preceptivo a un órgano de la Unión Europea y la notificación del pronunciamiento de ese órgano de la Unión Europea a la Administración instructora de acuerdo con lo previsto en el artículo 22.1.b) de la Ley 39/2015, de 1 de octubre.

d) La existencia, desde que se tenga constancia de la misma, de un procedimiento no finalizado en el ámbito de la Unión Europea que condicione directamente el contenido de la resolución, así como la finalización de dicho procedimiento de acuerdo con lo previsto en el artículo 22.1.c) de la Ley 39/2015, de 1 de octubre.

e) La solicitud de un informe preceptivo a un órgano de la misma o distinta Administración y la recepción, en su caso, de dicho informe, de acuerdo con lo previsto en el artículo 22.1.d) de la Ley 39/2015, de 1 de octubre.

f) La solicitud de previo pronunciamiento de un órgano jurisdiccional, cuando este sea indispensable para la resolución del procedimiento, así como el contenido del pronunciamiento cuando la Administración actuante tenga la constancia del mismo de acuerdo con lo previsto en el artículo 22.1.g) de la Ley 39/2015, de 1 de octubre.

g) La realización del requerimiento de anulación o revisión de actos entre administraciones previsto en el artículo 22.2.a) de la Ley 39/2015, de 1 de octubre, así como su cumplimiento o, en su caso, la resolución del correspondiente recurso contencioso-administrativo.

**Artículo 42.** *Práctica de las notificaciones a través de medios electrónicos.*

1. De acuerdo con lo previsto en el artículo 43.1 de la Ley 39/2015, de 1 de octubre, las notificaciones por medios electrónicos se practicarán mediante comparecencia en la sede electrónica o sede electrónica asociada de la Administración, organismo público o entidad de derecho público vinculado o dependiente actuante, a través de la Dirección Electrónica Habilitada única o mediante ambos sistemas, según disponga cada Administración, organismo público o entidad de derecho público vinculado o dependiente, debiendo quedar constancia de la fecha y hora del acceso al contenido de la misma, o del rechazo de la notificación.

En caso de que la Administración, organismo o entidad actuante lleve a cabo la puesta a disposición de las notificaciones por ambos sistemas, para el cómputo de plazos y el resto de efectos jurídicos se tomará la fecha y hora de acceso al contenido o el rechazo de la notificación por el interesado o su representante en el sistema en el que haya ocurrido en primer lugar. A tal efecto se habrá de disponer de los medios electrónicos necesarios para sincronizar de forma automatizada en uno y otro sistema la información sobre el estado de la notificación con objeto de garantizar la eficacia y seguridad jurídica en la tramitación del procedimiento.

2. Con independencia de que un interesado no esté obligado a relacionarse electrónicamente con las Administraciones Públicas o de que no haya comunicado que se le practiquen notificaciones por medios electrónicos, su comparecencia voluntaria o la de su representante en la sede electrónica o sede asociada de una Administración, organismo público o entidad de derecho público vinculado o dependiente o a través de la Dirección Electrónica Habilitada única, y el posterior acceso al contenido de la notificación o el rechazo expreso de esta tendrá plenos efectos jurídicos.

3. La notificación por comparecencia en la sede electrónica o sede electrónica asociada y a través de la Dirección Electrónica Habilitada única conlleva la puesta a disposición del interesado de un acuse de recibo que permita justificar bien el acceso al contenido de la notificación, bien el rechazo del interesado a recibirla.

El acuse contendrá, como mínimo, la identificación del acto notificado y la persona destinataria, la fecha y hora en la que se produjo la puesta a disposición y la fecha y hora del acceso a su contenido o del rechazo.

4. En los supuestos de sucesión de personas físicas o jurídicas, inter vivos o mortis causa, la persona o entidad que sucede al interesado comunicará la sucesión al órgano competente de la tramitación del procedimiento de cuya existencia tenga conocimiento. Dicha comunicación deberá efectuarse tras la efectividad de la sucesión o desde la inscripción de la defunción en el Registro Civil, en el caso de fallecimiento de persona física.

El órgano responsable de la tramitación procederá, en su caso, en procedimientos no finalizados, a autorizar a la persona o entidad sucesora el acceso a las notificaciones electrónicas ya practicadas desde la fecha del hecho causante de la sucesión y a practicar a dicha persona o entidad sucesora las notificaciones electrónicas que se produzcan en lo sucesivo. En el caso en el que la persona física sucesora no estuviera obligada a relacionarse electrónicamente con la Administración y no opte por este cauce de relación, las notificaciones que se produzcan en lo sucesivo deberán practicarse en papel, sin perjuicio de la garantía de acceso al expediente completo.

La persona o entidad que suceda al interesado en un procedimiento del que conozca su existencia debe comunicar, conforme a lo expuesto en los párrafos anteriores, la sucesión a la Administración Pública a la que corresponda la tramitación de aquel, en el plazo de 15 días hábiles, desde el día siguiente al de la efectividad de la sucesión o desde la inscripción de la defunción en el Registro Civil, en el caso de fallecimiento de persona física. Si la persona o entidad sucesora efectúa la comunicación después de dicho plazo, los defectos en la práctica de notificaciones que se deriven de este incumplimiento, que hubieran acaecido con anterioridad a dicha comunicación, le serán imputables al interesado; dándose por cumplida por la Administración, a todos los efectos, la obligación de puesta a disposición de la notificación electrónica en la sede electrónica o sede electrónica asociada, a través de la Dirección Electrónica Habilitada única o ambas, según proceda, a la persona jurídica o persona física cuya sucesión el interesado no ha hecho valer.

5. Toda notificación cuyo emisor pertenezca al ámbito estatal a que se refiere el artículo 1.2 de este Reglamento se pondrá a disposición del interesado a través de la Dirección Electrónica Habilitada única, incluyendo el supuesto previsto en el artículo 42.1 de la Ley 39/2015, de 1 de octubre. Asimismo, los emisores de ámbito estatal podrán notificar en su sede electrónica o sede electrónica asociada de forma complementaria a la puesta a disposición en la Dirección Electrónica Habilitada única.

**Artículo 43.** *Aviso de puesta a disposición de la notificación.*

1. De acuerdo con lo previsto en el artículo 41.6 de la Ley 39/2015, de 1 de octubre, con independencia de que la notificación se realice en papel o por medios electrónicos, las Administraciones Públicas, organismos públicos o entidades de derecho público vinculados o dependientes enviarán al interesado o, en su caso, a su representante, aviso informándole de la puesta a disposición de la notificación bien en la Dirección Electrónica Habilitada única, bien en la sede electrónica o sede electrónica asociada de la Administración, u Organismo o Entidad o, en su caso, en ambas.

La falta de práctica de este aviso, de carácter meramente informativo, no impedirá que la notificación sea considerada plenamente válida.

El aviso se remitirá al dispositivo electrónico o la dirección de correo electrónico que el interesado haya comunicado voluntariamente al efecto, o a ambos, de acuerdo con lo previsto en el artículo 41.1 de la Ley 39/2015, de 1 de octubre.

El interesado se hace responsable, por la comunicación a la Administración, organismo público o entidad de derecho público vinculado o dependiente, de que dispone de acceso al dispositivo o dirección de correo electrónico designados. En caso de que dejen de estar operativos o pierda la posibilidad de acceso, el interesado está obligado a comunicar a la Administración que no se realice el aviso en tales medios. El incumplimiento de esta obligación por parte del interesado no conllevará responsabilidad alguna para la Administración por los avisos efectuados a dichos medios no operativos.

El aviso regulado en este apartado sólo se practicará en caso de que el interesado o su representante hayan comunicado a la Administración un dispositivo electrónico o dirección de correo electrónico al efecto.

2. Cuando el interesado sea un sujeto obligado a relacionarse por medios electrónicos y la Administración emisora de la notificación no disponga de datos de contacto electrónicos para practicar el aviso de su puesta a disposición, en los procedimientos iniciados de oficio la primera notificación que efectúe la Administración, organismo o entidad se realizará en papel en la forma determinada por el artículo 42.2 de la Ley 39/2015, de 1 de octubre, advirtiendo al interesado en esa primera notificación que las sucesivas se practicarán en forma electrónica por comparecencia en la sede electrónica o sede electrónica asociada que corresponda o, en su caso, a través de la Dirección Electrónica Habilitada única según haya dispuesto para sus notificaciones la Administración, organismo o entidad respectivo, y dándole a conocer que, de acuerdo con lo previsto en el artículo 41.1 de la Ley 39/2015, de 1 de octubre, puede identificar un dispositivo electrónico, una dirección de correo electrónico o ambos para el aviso de la puesta a disposición de las notificaciones electrónicas posteriores.

3. Las Administraciones podrán crear bases de datos de contacto electrónico para la práctica de los avisos de puesta a disposición de notificaciones en su respectivo ámbito.

**Artículo 44.** *Notificación a través de la Dirección Electrónica Habilitada única.*

1. La Dirección Electrónica Habilitada única es el sistema de información para la notificación electrónica cuya gestión corresponde al Ministerio de Asuntos Económicos y Transformación Digital en colaboración con el Ministerio de Política Territorial y Función Pública.

2. De acuerdo con lo previsto en el artículo 7.4, la Dirección Electrónica Habilitada única se aloja en la sede electrónica del PAGe de la Administración General del Estado.

3. La adhesión a la Dirección Electrónica Habilitada única se realizará en los términos previstos en el artículo 65.

Todas las Administraciones Públicas y sus organismos públicos y entidades de derecho público vinculados o dependientes colaborarán para establecer sistemas interoperables que

permitan que las personas físicas y jurídicas puedan acceder a todas sus notificaciones a través de la Dirección Electrónica Habilitada única, tal como establece el artículo 43 de la Ley 39/2015, de 1 de octubre.

Esta previsión será aplicable con independencia de cuál sea la Administración que practica la notificación y si las notificaciones se han practicado en papel o por medios electrónicos.

4. Cuando una incidencia técnica imposibilite el funcionamiento ordinario de la Dirección Electrónica Habilitada única, una vez comunicada dicha incidencia a los órganos, organismos o entidades emisores que la utilicen como medio de notificación, estos podrán determinar una ampliación del plazo no vencido para comparecer y acceder a las notificaciones emitidas. En caso de que también pongan a disposición las notificaciones en su sede electrónica o sede electrónica asociada, deberán publicar también en esta tanto la incidencia técnica acontecida en la Dirección Electrónica Habilitada única como la ampliación concreta, en su caso, del plazo no vencido.

5. Con carácter previo al acceso al contenido de la notificación puesta a disposición del interesado en la Dirección Electrónica Habilitada única, este será informado de que de acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, dicho acceso al contenido, el rechazo expreso de la notificación o bien la presunción de rechazo por haber transcurrido el plazo de diez días naturales desde la puesta a disposición de la notificación sin acceder al contenido de la misma, dará por efectuado el trámite de notificación y se continuará el procedimiento.

6. Para dar por efectuado el trámite de notificación a efectos jurídicos, en la Dirección Electrónica Habilitada única deberá quedar constancia, con indicación de fecha y hora, del momento del acceso al contenido de la notificación, del rechazo expreso de la misma o del vencimiento del plazo previsto en el artículo 43.2 de la Ley 39/2015, de 1 de octubre.

El estado del trámite de notificación en la Dirección Electrónica Habilitada única se sincronizará automáticamente con la sede electrónica o sede electrónica asociada en la que, en su caso, la notificación también se hubiera puesto a disposición del interesado.

**Artículo 45.** *Notificación electrónica en sede electrónica o sede electrónica asociada.*

1. Con carácter previo al acceso al contenido de la notificación puesta a disposición del interesado en la sede electrónica o sede electrónica asociada del emisor de la misma, este será informado de que de acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, la comparecencia y acceso al contenido, el rechazo expreso de la notificación o bien la presunción de rechazo por haber transcurrido el plazo de diez días naturales desde la puesta a disposición de la notificación sin acceder al contenido de la misma dará por efectuado el trámite de notificación y se continuará el procedimiento.

2. Para dar por efectuado el trámite de notificación a efectos jurídicos, en la sede electrónica o sede electrónica asociada deberá quedar constancia, con indicación de fecha y hora, del momento del acceso al contenido de la notificación, del rechazo expreso de la misma o del vencimiento del plazo previsto en el artículo 43.2 de la Ley 39/2015, de 1 de octubre.

El estado del trámite de notificación en la sede electrónica o sede electrónica asociada se sincronizará automáticamente con la Dirección Electrónica Habilitada única si la notificación también se hubiera puesto a disposición del interesado en aquella.

3. De conformidad con el artículo 43.3 de la Ley 39/2015, de 1 de octubre, se entenderá cumplida la obligación de notificar en plazo por parte de la Administración, a que se refiere el artículo 40.4 de dicha ley, con la puesta a disposición de la notificación en la sede o en la dirección electrónica habilitada única.

TÍTULO III

## Expediente administrativo electrónico

CAPÍTULO I

### Documento administrativo electrónico y copias

**Artículo 46.** *Documento administrativo electrónico.*

1. Se entiende por documento administrativo electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico, según un formato determinado y susceptible de identificación y tratamiento diferenciado admitido en el Esquema Nacional de Interoperabilidad y normativa correspondiente, y que haya sido generada, recibida o incorporada por las Administraciones Públicas en el ejercicio de sus funciones sujetas a Derecho administrativo.

2. Cuando en el marco de un procedimiento administrativo tramitado por medios electrónicos el órgano actuante esté obligado a facilitar al interesado un ejemplar de un documento administrativo electrónico, dicho documento se podrá sustituir por la entrega de los datos necesarios para su acceso por medios electrónicos adecuados.

**Artículo 47.** *Requisitos de validez y eficacia de las copias auténticas de documentos.*

1. De acuerdo con lo previsto en el artículo 27.2 de la Ley 39/2015, de 1 de octubre, tendrá la consideración de copia auténtica de un documento público administrativo o privado original o de otra copia auténtica, la realizada, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido.

2. Las copias auténticas se expedirán siempre a partir de un original o de otra copia auténtica y tendrán la misma validez y eficacia que los documentos originales.

**Artículo 48.** *Órganos competentes para la emisión de copias auténticas de documentos en el ámbito estatal.*

1. En el ámbito estatal, serán competentes para la expedición de copias auténticas de documentos públicos administrativos o documentos privados, que sean documentos originales o copias auténticas de documento original los siguientes órganos:

a) Los órganos a los que corresponda la emisión de los documentos originales.
b) Los órganos a los que corresponda la custodia y archivo de documentos.
c) Los órganos que hayan previsto sus normas de competencia.
d) Las oficinas de asistencia en materia de registros, respecto de los documentos originales o copias auténticas presentados por las personas interesadas para que se remitan desde la Oficina a la unidad competente para su incorporación a un expediente administrativo.

2. La expedición de copias auténticas de documentos públicos administrativos o documentos privados, que sean documentos originales o copias auténticas de documento original, podrá llevarse a cabo mediante actuación administrativa automatizada o por personal funcionario habilitado inscrito en el Registro de Funcionarios Habilitados de la Administración General del Estado al que se refiere el artículo 31 de este Reglamento.

3. Los titulares de los órganos que se relacionan en los párrafos a), b) c) y d) del apartado 1 de este artículo designarán a los funcionarios y funcionarias habilitados para la emisión de las copias electrónicas auténticas, que se llevará a cabo mediante el correspondiente proceso de digitalización.

**Artículo 49.** *Emisión de copias de documentos aportados en papel por el interesado.*

Cuando el interesado presente en papel una copia de un documento público administrativo o de un documento privado para incorporarlo a un expediente administrativo,

el proceso de digitalización por la Administración Pública generará una copia electrónica que tendrá el mismo valor que la copia presentada en papel.

**Artículo 50.** *Referencia temporal de los documentos administrativos electrónicos.*

1. Todos los documentos administrativos electrónicos deberán llevar asociadas una de las siguientes modalidades de referencia temporal, de acuerdo con lo que determinen las normas reguladoras de los respectivos procedimientos:

a) Marca de tiempo, entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

b) Sello electrónico cualificado de tiempo, entendiendo por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador cualificado de servicios de confianza que asegure la exactitud e integridad de la marca de tiempo del documento. Los sellos electrónicos de tiempo no cualificados serán asimilables a todos los efectos a las marcas de tiempo.

2. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello electrónico cualificado de tiempo

La información relativa a las marcas y sellos electrónicos cualificados de tiempo se asociará a los documentos electrónicos en la forma que determine el Esquema Nacional de Interoperabilidad y normativa correspondiente.

3. La relación de prestadores cualificados de servicios de confianza que prestan servicios de sellado de tiempo en el sector público deberá estar incluida en la «Lista de confianza de prestadores cualificados de servicios de confianza».

**Artículo 51.** *Configuración del expediente administrativo electrónico.*

1. El foliado de los expedientes administrativos electrónicos se llevará a cabo mediante un índice electrónico autenticado que garantizará la integridad del expediente y permitirá su recuperación siempre que sea preciso.

2. Un mismo documento electrónico podrá formar parte de distintos expedientes administrativos.

3. El índice electrónico autenticado será firmado por el titular del órgano que conforme el expediente para su tramitación o bien podrá ser sellado electrónicamente en el caso de expedientes electrónicos que se formen de manera automática, a través de un sistema que garantice su integridad.

**Artículo 52.** *Ejercicio del derecho de acceso al expediente electrónico y obtención de copias de los documentos electrónicos.*

De acuerdo con lo previsto en el artículo 53.1.a) de la Ley 39/2015, de 1 de octubre, el derecho de acceso de las personas interesadas que se relacionen electrónicamente con las Administraciones Públicas al expediente electrónico y, en su caso, a la obtención de copia total o parcial del mismo, se entenderá satisfecho mediante la puesta a disposición de dicho expediente en el Punto de Acceso General electrónico de la Administración competente o en la sede electrónica o sede electrónica asociada que corresponda.

A tal efecto, la Administración destinataria de la solicitud remitirá al interesado o, en su caso a su representante, la dirección electrónica o localizador que dé acceso al expediente electrónico puesto a disposición, garantizando aquella el acceso durante el tiempo que determine la correspondiente política de gestión de documentos electrónicos siempre de acuerdo con el dictamen de valoración emitido por la autoridad calificadora correspondiente, y el cumplimiento de la normativa aplicable en materia de protección de datos de carácter personal y de transparencia y acceso a la información pública y de patrimonio documental, histórico y cultural.

**Artículo 53.** *Tiempo de conservación y destrucción de documentos.*

1. Los documentos presentados por el interesado en soporte papel que por cualquier circunstancia no le puedan ser devueltos en el momento de su presentación, una vez digitalizados serán conservados a su disposición durante seis meses para que pueda

recogerlos, independientemente del procedimiento administrativo al que se incorporen o de la Administración Pública a que vayan dirigidos, salvo que reglamentariamente la Administración correspondiente establezca un plazo mayor.

2. Los documentos presentados por el interesado en formato electrónico dentro de un dispositivo, que por cualquier circunstancia no le puedan ser devueltos en el momento de su presentación, una vez incorporados al expediente serán conservados a su disposición durante seis meses para que pueda recogerlos, independientemente del procedimiento administrativo al que se incorporen o de la Administración Pública a que vayan dirigidos, salvo que reglamentariamente la Administración correspondiente establezca un plazo mayor.

3. Transcurrido el plazo previsto en los apartados anteriores, la destrucción de los documentos se realizará de acuerdo con las competencias del Ministerio de Cultura y Deporte o del órgano competente de la comunidad autónoma, y siempre que no se trate de documentos con valor histórico, artístico u otro relevante o de documentos en los que la firma u otras expresiones manuscritas o mecánicas confieran al documento un valor especial.

4. Cuando la generación de copias electrónicas auténticas se realice a partir de documentos originales o copias auténticas de documentos en soporte no electrónico que se conserven formando parte de sus correspondientes expedientes y series documentales en cualesquiera de las oficinas, archivos o dependencias de cualquier organismo de las Administraciones públicas, dichos documentos originales o copias auténticas de documentos en soporte no electrónico se restituirán a sus oficinas, archivos o dependencias de origen, donde les será de aplicación la normativa específica en materia de archivos y conservación del patrimonio documental en su respectivo ámbito y siguiendo lo establecido por las autoridades calificadoras que correspondan.

5. En el ámbito estatal, se estará a lo preceptuado en el Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y entidades de derecho público y la conservación de documentos administrativos en soporte distinto al original.

## CAPÍTULO II

## Archivo electrónico de documentos

**Artículo 54.** *Conservación de documentos electrónicos.*

1. De acuerdo con lo previsto en el artículo 46 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas, así como sus organismos públicos y entidades de derecho público vinculados o dependientes, deberán conservar en soporte electrónico todos los documentos que formen parte de un expediente administrativo y todos aquellos documentos con valor probatorio creados al margen de un procedimiento administrativo.

La copia electrónica auténtica generada conforme a lo dispuesto en el artículo 27 de la Ley 39/2015, de 1 de octubre, tiene la consideración de patrimonio documental a efectos de aplicación de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español o la normativa autonómica correspondiente, siendo el periodo de conservación de los documentos el establecido por las autoridades calificadoras que correspondan.

2. Cada Administración Pública, regulará los períodos mínimos de conservación de los documentos electrónicos, que formen parte del expediente de un procedimiento cuya tramitación haya concluido, conforme a su normativa específica de archivos y patrimonio documental.

Cuando se tenga conocimiento por la Administración Pública, organismo o entidad de la existencia de procedimientos judiciales que afecten o puedan afectar a documentos electrónicos, estos deberán conservarse a disposición de los órganos jurisdiccionales, hasta tanto exista constancia de la terminación del procedimiento judicial correspondiente en las sucesivas instancias, por haber recaído resolución no susceptible de recurso o procedimiento alguno ante órganos jurisdiccionales nacionales o internacionales.

3. La conservación de los documentos electrónicos deberá realizarse de forma que permita su acceso y comprenda, como mínimo, su identificación, contenido, metadatos, firma, estructura y formato.

También será posible la inclusión de su información en bases de datos siempre que, en este último caso, consten los criterios para la reconstrucción de los formularios o modelos electrónicos origen de los documentos, así como para la comprobación de la identificación o firma electrónica de dichos datos.

Los plazos de conservación de esta información están sujetos a los mismos plazos establecidos para los correspondientes documentos electrónicos.

4. Para asegurar la conservación, acceso y consulta de los documentos electrónicos archivados con independencia del tiempo transcurrido desde su emisión, se podrán trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones, de acuerdo con lo previsto en el artículo 27 de la Ley 39/2015, de 1 de octubre y en la normativa específica de archivos y patrimonio documental, histórico y cultural.

Asimismo, se planificarán las actuaciones de preservación digital que garanticen la conservación a largo plazo de los documentos digitales y permitan de esta forma dar cumplimiento a lo establecido en el párrafo anterior

5. En todo caso, bajo la supervisión de los responsables de la seguridad y de los responsables de la custodia y gestión del archivo electrónico y de los responsables de las unidades productoras de la documentación se establecerán los planes y se habilitarán los medios tecnológicos para la migración de los datos a otros formatos y soportes que permitan garantizar la autenticidad, integridad, disponibilidad, conservación y acceso al documento cuando el formato de los mismos deje de figurar entre los admitidos por el Esquema Nacional de Interoperabilidad y normativa correspondiente.

**Artículo 55.** *Archivo electrónico único.*

1. El archivo electrónico único de cada Administración es el conjunto de sistemas y servicios que sustenta la gestión, custodia y recuperación de los documentos y expedientes electrónicos así como de otras agrupaciones documentales o de información una vez finalizados los procedimientos administrativos o actuaciones correspondientes.

2. En el archivo electrónico único de la Administración General del Estado serán accesibles todos los documentos y expedientes electrónicos del sector público estatal una vez finalizados los procedimientos y en los plazos determinados por la Comisión Superior Calificadora de Documentos Administrativos de acuerdo con lo que se desarrolle reglamentariamente.

La gestión del archivo electrónico único garantizará la autenticidad, conservación, integridad, confidencialidad, disponibilidad y cadena de custodia de los expedientes y documentos almacenados, así como su acceso, en las condiciones exigidas por el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad, por la normativa de transparencia, acceso a la información pública y buen gobierno, por la legislación de archivos y patrimonio histórico y cultural y por la normativa específica que sea de aplicación, de acuerdo con lo que se desarrolle reglamentariamente.

## TÍTULO IV

## De las relaciones y colaboración entre las Administraciones Públicas para el funcionamiento del sector público por medios electrónicos

### CAPÍTULO I

### Colaboración entre las Administraciones Públicas para la actuación administrativa por medios electrónicos

**Artículo 56.** *Relaciones interadministrativas e interorgánicas por medios electrónicos.*

De acuerdo con lo previsto en el artículo 3.2 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas, en el ejercicio de sus competencias, estarán obligadas a

relacionarse a través de medios electrónicos entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes.

Esta misma obligación será de aplicación a las entidades de derecho privado vinculadas o dependientes de las Administraciones públicas cuando actúen en el ejercicio de potestades administrativas.

**Artículo 57.** *Comunicaciones en la Administración General del Estado.*

Los órganos de la Administración General del Estado y los organismos públicos y entidades de derecho público vinculados o dependientes de esta deberán utilizar medios electrónicos para comunicarse entre sí.

Las comunicaciones se efectuarán a través del Registro Electrónico General de la Administración General del Estado o registro del organismo público o entidad de derecho público de que se trate, o por cualquier otro medio electrónico que permita dejar constancia de su recepción.

Esta misma obligación será de aplicación a las entidades de derecho privado vinculadas o dependientes de las Administraciones públicas cuando actúen en el ejercicio de potestades administrativas.

**Artículo 58.** *Adhesión a sedes electrónicas y sedes electrónicas asociadas.*

Las Administraciones Públicas y los organismos públicos y entidades de derecho público vinculados o dependientes podrán adherirse voluntariamente, mediante la formalización del correspondiente instrumento de adhesión, a las sedes electrónicas o sedes asociadas disponibles de titularidad de la misma Administración u otra Administración Pública, sin que se constituya como sede electrónica asociada.

**Artículo 59.** *Adhesión a la Carpeta Ciudadana del sector público estatal.*

Las Administraciones Públicas podrán integrar sus respectivas áreas personalizadas o carpetas ciudadanas a que se refiere el segundo párrafo del artículo 7.3 de este Reglamento, si las hubiere, o determinadas funcionalidades de las mismas, con la Carpeta Ciudadana prevista en el artículo 8 de este Reglamento, de forma que el interesado pueda acceder a sus contenidos o funcionalidades mediante procedimientos seguros que garanticen la integridad y confidencialidad de sus datos de carácter personal, independientemente de cuál haya sido su punto de acceso.

**Artículo 60.** *Sistema de interconexión de Registros.*

1. Las aplicaciones o sistemas de información para el tratamiento del Registro Electrónico General de cada Administración, así como del registro electrónico de cada organismo público o entidad de derecho público vinculado o dependiente, deberán ser interoperables.

2. Las interconexiones entre Registros de las Administraciones Públicas deberán realizarse a través del Sistema de Interconexión de Registros (SIR) gestionado por el Ministerio de Asuntos Económicos y Transformación Digital en colaboración con el Ministerio de Política Territorial y Función Pública de acuerdo con lo previsto en el Esquema Nacional de Interoperabilidad y en la correspondiente Norma Técnica.

3. En el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes las aplicaciones o sistemas de información para el tratamiento del Registro Electrónico General de la Administración General del Estado, así como del registro electrónico de cada organismo público o entidad de derecho público vinculado o dependiente, deberán permitir la interoperabilidad con los sistemas de gestión de expedientes de las unidades de tramitación correspondientes.

**Artículo 61.** *Transmisiones de datos.*

1. Las transmisiones de datos a las que se refiere el artículo 155 de la Ley 40/2015, de 1 de octubre, realizadas a través de redes corporativas de las Administraciones Públicas para el envío de documentos elaborados por cualquier Administración, mediante consulta a las

plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, tienen la consideración de certificados administrativos necesarios para el procedimiento o actuación administrativa.

2. Cuando las personas interesadas no aporten datos y/o documentos que ya obren en poder de las Administraciones Públicas, de conformidad con lo establecido en la Ley 39/2015, de 1 de octubre, se seguirán las siguientes reglas:

a) Si el órgano administrativo encargado de la tramitación del procedimiento, puede acceder electrónicamente a los datos, documentos o certificados necesarios mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, los incorporará al procedimiento administrativo correspondiente. Quedará constancia en los ficheros del órgano, organismo público o entidad de derecho público cedente del acceso a los datos o documentos efectuado por el órgano u organismo cesionario.

b) Excepcionalmente, en caso de que no se pueda realizar el acceso electrónico a los datos mediante la consulta a que se refiere la letra anterior, se podrá solicitar por otros medios habilitados al efecto y se conservará la documentación acreditativa de la circunstancia que imposibilitó dicho acceso electrónico, incorporándola al expediente.

3. Toda transmisión de datos se efectuará a solicitud del órgano o entidad tramitadora en la que se identificarán los datos requeridos y sus titulares, así como la finalidad para la que se requieren. Además, si en la petición de datos interviene un empleado o empleada público se incluirá la identificación de este en la petición.

4. El órgano, organismo público o entidad de derecho público cesionario será responsable del correcto acceso electrónico a los datos cuya titularidad corresponda a otro órgano, organismo público o entidad de derecho público, así como de su utilización, en particular, cuando los datos a los que se accede tengan un régimen de especial protección. Asimismo, cuando para dicho acceso se requiera el consentimiento del interesado, el cesionario será responsable del requerimiento de dicho consentimiento.

5. La cesión de datos dentro de una actuación administrativa podrá llevarse a cabo, entre otras formas, de manera automatizada, entendiéndose por tal la consulta realizada íntegramente a través de medios telemáticos en la que no haya intervenido de forma directa un empleado o empleada público.

6. Las transmisiones de datos que se realicen en virtud del artículo 14 del Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.º 1024/2012 no requerirán previsualización de los datos por parte del usuario o usuaria solicitante para proceder a su uso por parte del órgano o entidad tramitadora.

**Artículo 62.** *Plataformas de intermediación de datos.*

1. Las plataformas de intermediación de datos dejarán constancia de la fecha y hora en que se produjo la transmisión, así como del procedimiento administrativo, trámite o actuación al que se refiere la consulta. Las plataformas de intermediación, o sistema electrónico equivalente, existentes en el sector público deberán ser interoperables con la Plataforma de Intermediación de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes y entre ellas.

La adhesión a las plataformas de intermediación de datos requerirá que se garantice el cumplimiento de las condiciones de seguridad exigidas por los cedentes de la información para el tratamiento de datos por parte de la plataforma encargada del tratamiento de dichos datos y de los cesionarios de los mismos.

2. En el ámbito estatal, se dispondrá de la Plataforma de Intermediación de Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes a que se refiere la Ley 39/2015, de 1 de octubre. Dicha Plataforma será gestionada la Secretaría General de Administración Digital y actuará como un punto a través del cual cualquier órgano, organismo público o entidad de derecho público podrá consultar los datos o documentos asociados al procedimiento de que se trate, con

independencia de que la presentación de los citados datos o documentos tenga carácter preceptivo o facultativo en el procedimiento de que se trate.

3. La Plataforma de Intermediación de la Administración General del Estado actuará como punto de conexión con el sistema técnico regulado por el Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, para el intercambio automático de datos o documentos a nivel europeo.

**Artículo 63.** *Remisión electrónica de expedientes administrativos en el ámbito de las Administraciones públicas mediante puesta a disposición.*

1. Cuando desde una Administración Pública se solicite a otra un expediente electrónico, la remisión por esta, a través de un nodo de interoperabilidad, de la dirección electrónica o localizador que dé acceso al expediente electrónico puesto a disposición de la primera equivaldrá a la remisión del mismo, siempre que se garantice la integridad del acceso a lo largo del tiempo que determine la correspondiente política de gestión de documentos electrónicos y el cumplimiento de la normativa de interoperabilidad aplicable al tipo de expediente.

2. El mismo procedimiento previsto en el apartado anterior se podrá utilizar cuando la solicitud se produzca dentro del ámbito de una misma Administración Pública.

## CAPÍTULO II

## Transferencia y uso compartido de tecnologías entre Administraciones Públicas

**Artículo 64.** *Reutilización de sistemas y aplicaciones de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 157 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por estar previsto en una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.

2. A tal efecto, de acuerdo con lo previsto en el artículo 158 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas mantendrán directorios actualizados de aplicaciones para su libre reutilización en modo producto o en modo servicio, de conformidad con lo dispuesto en el Esquema Nacional de Interoperabilidad.

Estos directorios deberán ser plenamente interoperables, de modo que se garantice su compatibilidad informática e interconexión, con el Directorio general de aplicaciones de la Administración General del Estado para su libre reutilización previsto en el artículo 17 del Real Decreto 4/2010, de 8 de enero.

3. Las condiciones de licenciamiento de los sistemas y aplicaciones de las Administraciones públicas y el uso y funcionamiento de los directorios de aplicaciones reutilizables deberán ajustarse a lo previsto en el Real Decreto 4/2010, de 8 de enero.

4. Las Administraciones públicas procurarán la construcción de aplicaciones reutilizables, bien en modo producto o en modo servicio, con el fin de favorecer las actuaciones de compartir, reutilizar y colaborar, en beneficio de una mejor eficiencia y para atender de forma efectiva las solicitudes recibidas en virtud del artículo 157 de la Ley 40/2015, de 1 de octubre.

5. Las Administraciones Públicas, con carácter previo a la adquisición, desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación, tanto si se realiza con medios propios o por la contratación de los servicios correspondientes, deberán consultar en el Directorio general de aplicaciones de la Administración General del Estado para su libre reutilización, si existen soluciones disponibles para su reutilización, que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir, y siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

Las conclusiones con respecto al resultado de dicha consulta al directorio general se incorporarán en el expediente de contratación y reflejarán, en su caso, que no existen

soluciones disponibles para su reutilización que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir.

En el caso de existir una solución disponible para su reutilización total o parcial, la justificación de la no reutilización se realizará en términos de eficiencia conforme a lo establecido en el artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

**Artículo 65.** *Adhesión a las plataformas de la Administración General del Estado.*

1. La adhesión al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado prevista en la Ley 39/2015, de 1 de octubre, en la Ley 40/2015, de 1 de octubre, y en este Reglamento, así como a aquellos otros que puedan facilitar el cumplimiento de lo dispuesto en estas normas se realizará mediante adhesión por el órgano competente de la Administración Pública que corresponda, en el que se dejará constancia de la voluntad de este de adherirse a las plataformas, registros o servicios electrónicos y de aceptar en su integridad las condiciones de uso determinadas por el órgano titular de la plataforma o servicio, incluyendo el comienzo efectivo del mismo.

A tal efecto, los modelos de adhesión a las plataformas, registros o servicios, que incluirán los términos de prestación del servicio y de la contribución al sostenimiento del mismo, se aprobarán mediante Resolución de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital o, en su caso, del órgano directivo, organismo público o entidad de derecho público que sea competente de las plataformas, registros o servicios de que se trate.

2. La adhesión a una plataforma, registro o servicio electrónico de la Administración General del Estado no supondrá un cambio de la titularidad sobre las actuaciones administrativas realizadas en el procedimiento administrativo de que se trate, que corresponderá a la Administración competente para su tramitación. Si la plataforma provee un servicio que requiere el intercambio de información entre dos entidades usuarias de la misma o de distinta plataforma, la autenticación de la entidad solicitante puede acreditarse, ante la entidad cedente, mediante un sello electrónico cualificado del órgano, organismo público o entidad de derecho público que gestiona la plataforma en cuestión de la que es usuaria la entidad solicitante, que actuará en nombre de los órganos y organismos o entidades adheridos que actúan como solicitantes.

La adhesión a una plataforma de la Administración General del Estado requerirá que se cumplan las condiciones de seguridad exigidas por los cedentes de la información.

3. Los órganos competentes para la gestión del procedimiento administrativo de las Administraciones que se adhieran a estas plataformas, registros o servicios electrónicos se responsabilizarán del uso que hagan de las mismas en el ejercicio de sus competencias, correspondiendo al órgano responsable de la plataforma su gestión y mantenimiento. En el supuesto de que una incidencia técnica imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, y sin perjuicio de la ampliación de plazos a que se refiere el artículo 32.4 de la Ley 39/2015, de 1 de octubre, cada Administración pública será responsable de la continuación de la tramitación de sus procedimientos administrativos y servicios a la ciudadanía.

4. La adhesión de las comunidades autónomas o entidades locales a las plataformas estatales o registros previstos en la disposición adicional segunda de la Ley 39/2015, de 1 de octubre, es voluntaria, si bien la no adhesión deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, para lo que se enviará el correspondiente informe al Ministerio de Asuntos Económicos y Transformación Digital, en el que deberá incluirse la justificación del cumplimiento de los requisitos del Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad y sus normas técnicas de desarrollo, de plataformas, registros o servicios electrónicos que se utilicen, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes plataformas.

**Disposición adicional primera.** *Obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado.*

Las personas participantes en procesos selectivos convocados por la Administración General del Estado, sus organismos públicos o entidades de derecho público vinculados o dependientes a la misma, deberán realizar la presentación de las solicitudes y documentación y, en su caso, la subsanación y los procedimientos de impugnación de las actuaciones de estos procesos selectivos a través de medios electrónicos.

**Disposición adicional segunda.** *Formación de empleados y empleadas públicos de la Administración General del Estado.*

La Administración General del Estado promoverá la formación del personal a su servicio para garantizar el derecho de las personas interesadas a ser asistidas en el uso de medios electrónicos en sus relaciones con la Administración Pública, establecido en la Ley 39/2015, de 1 de octubre.

**Disposición adicional tercera.** *Nodo de interoperabilidad de identificación electrónica del Reino de España.*

1. Se crea el nodo de interoperabilidad de identificación electrónica del Reino de España para el reconocimiento mutuo de identidades electrónicas entre los Estados miembros, de acuerdo con lo previsto en el Reglamento (UE) n.º 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
2. El nodo de interoperabilidad de identificación electrónica del Reino de España se gestionará por el Ministerio de Asuntos Económicos y Transformación Digital.
3. Las entidades pertenecientes al sector público deberán definir y publicar en su sede electrónica el nivel de seguridad en la identificación electrónica exigido en los procedimientos y servicios que gestionan, de acuerdo con el Reglamento (UE) n.º 910/2014, de 23 de julio de 2014. Este nivel de seguridad en la identificación electrónica del sistema de información que soporta el procedimiento o servicio se determinará sobre la base del análisis de riesgos, de acuerdo con el Esquema Nacional de Seguridad y normativa correspondiente.
4. Las entidades pertenecientes al sector público deberán admitir en todo caso, en el acceso electrónico a sus procedimientos y servicios los esquemas de identificación notificados por otros Estados Miembros al amparo del Reglamento (UE) n.º 910/2014, de 23 de julio de 2014, siempre que se den estas dos condiciones:

a) El esquema de identificación utilizado tenga un nivel de seguridad en la identificación electrónica sustancial o alto.
b) El nivel de seguridad de dicho esquema sea igual o superior al nivel de seguridad exigido por el procedimiento o servicio de acuerdo con el apartado 3.

**Disposición adicional cuarta.** *Adhesión de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado en el ejercicio de potestades administrativas a las sedes electrónicas y sedes electrónicas asociadas y sistema de firma y notificaciones electrónicas aplicables.*

De acuerdo con lo previsto en el artículo 2.2.b) de la Ley 39/2015, de 1 de octubre, y el artículo 2.2.b) de la Ley 40/2015, de 1 de octubre, cuando las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado ejerzan potestades administrativas y, en consecuencia, les sea de aplicación este Reglamento, se observarán las siguientes disposiciones:

a) De acuerdo con lo previsto en el artículo 58, las entidades de derecho privado tendrán que adherirse a la sede electrónica asociada del ministerio con el que mantengan la vinculación o dependencia o, en su caso, a la sede electrónica o sede electrónica asociada del organismo de derecho público con el que mantengan la misma, en ambos casos mediante la formalización del correspondiente instrumento de adhesión.

Las personas interesadas obligadas a relacionarse electrónicamente con las entidades de derecho privado en el ejercicio de dichas potestades realizarán los trámites del procedimiento mediante los modelos normalizados que estarán disponibles en la sede electrónica asociada o, en su caso, sede electrónica a la que se haya adherido la entidad. El mismo régimen se aplicará a los sujetos no obligados que hayan optado por medios electrónicos de acuerdo con lo previsto en el artículo 3 de este Reglamento.

b) Según lo previsto en los artículos 20.2 y 22.4, mediante orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se determinarán reglamentariamente los medios admitidos para la firma electrónica en los procedimientos tramitados en el ejercicio de potestades administrativas por parte de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado.

c) De conformidad con lo previsto en el artículo 42, las notificaciones electrónicas que las entidades de derecho privado tengan que practicar se llevarán a cabo en la misma forma que el responsable de la sede electrónica asociada o sede electrónica a la que esté adherida la entidad haya dispuesto para sus propias notificaciones.

**Disposición adicional quinta.** *Adhesión de los órganos constitucionales al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado.*

1. Sin perjuicio de lo previsto en el artículo 65 de este Reglamento, los órganos constitucionales podrán adherirse al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado y aquellos otros que puedan facilitar el cumplimiento de lo dispuesto en la Ley 39/2015, de 1 de octubre, en la Ley 40/2015, de 1 de octubre, y en este Reglamento.

2. La adhesión se realizará mediante un acuerdo o acto de adhesión en el que la autoridad competente de las instituciones u órganos anteriores dejará constancia de la voluntad de este de adherirse a las plataformas, registros o servicios electrónicos y de aceptar en su integridad las condiciones de uso determinadas por el órgano titular de la plataforma o servicio, incluyendo el comienzo efectivo del mismo.

Para el estudio de su viabilidad, remitirá con carácter previo al Ministerio al que pertenezca el órgano titular de la plataforma o servicio una memoria justificativa y económica en que se explicite el volumen de trámites que estaría previsto realizar a través de la plataforma, el registro o servicio electrónico de que se trate, los efectos presupuestarios y económicos y cualquier otra razón de interés general que justifique su adhesión.

3. La adhesión a una plataforma, registro o servicio electrónico de la Administración General del Estado no supondrá un cambio de la titularidad sobre las actuaciones administrativas realizadas en el procedimiento administrativo de que se trate, que corresponderá a la Administración competente para su tramitación.

Si la plataforma, registro o servicio electrónico provee un servicio que requiere el intercambio de información entre dos entidades usuarias de la misma o distinta plataforma, la autenticación de la entidad solicitante puede acreditarse ante la entidad cedente mediante un sello electrónico cualificado del órgano, organismo público o entidad de derecho público que gestiona la plataforma.

4. La adhesión a una plataforma de la Administración General del Estado requerirá que se cumplan las condiciones de seguridad exigidas por los cedentes de la información.

5. Los órganos competentes en las instituciones u órganos adheridos se responsabilizarán del uso que hagan de las plataformas en el ejercicio de sus competencias, correspondiendo al órgano responsable de la plataforma su gestión y mantenimiento. En el supuesto de una incidencia técnica imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, los órganos competentes en las instituciones u órganos adheridos serán responsables de la continuación de la tramitación de sus procedimientos administrativos.

**Disposición adicional sexta.** *Situación de las sedes electrónicas y subsedes electrónicas en el ámbito estatal existentes a la entrada en vigor de este real decreto.*

1. En aplicación de lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, las sedes electrónicas existentes en la Administración General del Estado en la fecha de entrada en vigor de este real decreto pasan a tener naturaleza de sedes electrónicas

asociadas de la sede electrónica de la Administración General del Estado, que es la sede del Punto de Acceso General electrónico (PAGe) de la Administración General del Estado, sin necesidad de modificar su instrumento de creación. Las subsedes electrónicas existentes en la fecha de entrada en vigor de este real decreto pasarán también a tener naturaleza de sedes electrónicas asociadas.

2. Las sedes electrónicas de los organismos públicos o entidades de derecho público vinculados o dependientes existentes en la fecha de entrada en vigor de este real decreto mantendrán su naturaleza de sede electrónica. Las subsedes electrónicas de estos pasarán a tener naturaleza de sedes electrónicas asociadas.

**Disposición adicional séptima.** *Interoperabilidad de los registros electrónicos de apoderamientos.*

1. En aplicación de lo previsto en el artículo 6 de la Ley 39/2015, de 1 de octubre, y el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, la Norma Técnica de Interoperabilidad establecerá el modelo de datos y las condiciones de interoperabilidad de los registros electrónicos de apoderamientos, abordando los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, a los registros mercantiles, de la propiedad y a los protocolos notariales.

2. En el ámbito de la Administración General del Estado, el cumplimiento de las previsiones del artículo 33.2 del Reglamento sobre el acceso al Registro Electrónico de Apoderamientos de la Administración General del Estado está vinculado a la aprobación y aplicación de la Norma Técnica a que se refiere el apartado 1 anterior.

**Disposición adicional octava.** *Supletoriedad en Registro Civil.*

De conformidad con lo dispuesto en el artículo 88 y en la Disposición final primera de la Ley 20/2011, de 21 de julio, del Registro Civil, este Reglamento será de aplicación supletoria en lo no previsto en dicha Ley y su normativa de desarrollo específica, en cuanto a todo lo relacionado con la tramitación administrativa de los procedimientos específicos de Registro Civil.

**Disposición adicional novena.** *Autorización de los sistemas de identificación previstos en el artículo 9.2.c) y de los sistemas de firma previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre.*

1. Los sistemas de identificación a que se refiere el artículo 9.2.c) y los sistemas de firma a que se refiere el artículo 10.2.c) de la ley 39/2015, de 1 de octubre, que, en ambos casos, se hubieran puesto en servicio hasta el 6 de noviembre de 2019, fecha de entrada en vigor de la modificación de dichos artículos en virtud del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, no requerirán la autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior, siempre y cuando no hayan sido modificados tras dicha fecha.

2. Los sistemas que, tras el 6 de noviembre de 2019, hayan sido autorizados en aplicación de las previsiones de los artículos 9.2.c) y 10.2.c) de la Ley 39/2015, de 1 de octubre, y sean modificados posteriormente, deberán ser objeto de una nueva autorización previa a su puesta en servicio.

**Disposición adicional décima.** *Especialidades por razón de materia.*

1. De acuerdo con la disposición adicional primera de la Ley 39/2015, de 1 de octubre, los procedimientos administrativos regulados en leyes especiales por razón de la materia que no exijan alguno de los trámites previstos en la citada ley o regulen trámites adicionales o distintos se regirán, respecto a estos, por lo dispuesto en dichas leyes especiales.

2. Las siguientes actuaciones y procedimientos se regirán por su normativa específica y supletoriamente por lo dispuesto en la Ley 39/2015, de 1 de octubre:

a) Las actuaciones y procedimientos de aplicación de los tributos en materia tributaria y aduanera, así como su revisión en vía administrativa.

b) Las actuaciones y procedimientos de gestión, inspección, liquidación, recaudación, impugnación y revisión en materia de Seguridad Social y desempleo.

c) Las actuaciones y procedimientos sancionadores en materia tributaria y aduanera, en el orden social, en materia de tráfico y seguridad vial y en materia de extranjería.

d) Las actuaciones y procedimientos en materia de extranjería y asilo.

3. De acuerdo con lo previsto en la Disposición adicional decimoséptima de la Ley 40/2015, de 1 de octubre, la Agencia Estatal de Administración Tributaria se regirá por su legislación específica y únicamente de forma supletoria y en tanto resulte compatible con su legislación específica por lo previsto en dicha Ley. El acceso, la cesión o la comunicación de información de naturaleza tributaria se regirán en todo caso por su legislación específica.

**ANEXO**

**Definiciones**

– Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otras personas usuarias.

– Archivo electrónico único de cada Administración: Conjunto de sistemas y servicios que sustente la gestión, custodia y recuperación de los documentos y expedientes electrónicos así como de otras agrupaciones documentales o de información una vez finalizados los procedimientos o actuaciones correspondientes.

– Autenticación: Procedimiento de verificación de la identidad digital de un sujeto en sus interacciones en el ámbito digital, típicamente mediante factores tales como «algo que se sabe»(contraseñas o claves concertadas), «algo que se tiene» sean componentes lógicos (como certificados software) o dispositivos físicos (en expresión inglesa, tokens), o «algo que se es» (elementos biométricos), factores utilizados de manera aislada o combinados.

– Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Canal: Estructura o medio de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, etc.).

– Certificado electrónico: Documento emitido y firmado por la Autoridad de Certificación que identifica una clave pública con su propietario. Cada certificado está identificado por un número de serie único y tiene un periodo de validez que está incluido en el certificado.

– Certificado cualificado: Un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

– Certificado cualificado de sello electrónico: Certificado de sello electrónico que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

– Código malicioso: Tipo de software de carácter dañino que crea o aprovecha vulnerabilidades en dispositivos, sistemas y archivos informáticos que permiten el acceso remoto no autorizado, la generación de puertas traseras, el robo o exfiltración de datos, la destrucción de información, u otras acciones perjudiciales.

– Código Seguro de Verificación (CSV): Código que identifica a un documento electrónico y cuya finalidad es garantizar el origen e integridad de los documentos mediante

el acceso a la sede electrónica correspondiente; el carácter único del código generado para cada documento; su vinculación con el documento generado, de forma que cualquier modificación del documento generado dará lugar a un nuevo documento con un código seguro de verificación diferente; la posibilidad de verificar el documento en la sede electrónica como mínimo por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento; así como un acceso al documento restringido a quien disponga del código seguro de verificación.

– Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

– Copia auténtica: Tendrá la consideración de copia auténtica de un documento público administrativo o privado original o de otra copia auténtica, la realizada, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido

– Copia autorizada electrónica: documento notarial electrónico generado por el notario que autorizó la escritura, con el mismo valor y efectos que la copia en papel y al cual se le atribuye también valor de documento público.

– Digitalización: Proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento.

– Dirección electrónica: Identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones

– Directorio de aplicaciones reutilizables: instrumento que contiene la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

– Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

– Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

– Entorno cerrado de comunicación: escenario de comunicaciones delimitado, controlado y protegido en el que los participantes se relacionan a través de medios electrónicos, según unas garantías y condiciones determinadas que incluyen la relación de emisores y receptores autorizados, la naturaleza de los datos a intercambiar y las medidas de seguridad y protección de datos.

– Especificación técnica: Según el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea, documento en el que se prescriben los requisitos técnicos que debe reunir un producto, proceso, servicio o sistema y que establece uno o más de los aspectos siguientes:

• Las características que debe tener un producto, como los niveles de calidad, rendimiento, interoperabilidad, protección del medio ambiente, salud y seguridad y sus dimensiones, así como los requisitos aplicables al producto en lo que respecta a la denominación con la que se vende, la terminología, los símbolos, los ensayos y los métodos de ensayo, el embalaje, el marcado o el etiquetado y los procedimientos de evaluación de la conformidad;

• los métodos y procedimientos de producción de los productos agrícolas, definidos en el artículo 38, apartado 1, del TFUE, de los productos destinados a la alimentación humana y animal y de los medicamentos, así como los métodos y procedimientos de producción relacionados con los demás productos, en caso de que estos influyan en sus características;

• las características que debe tener un servicio, como los niveles de calidad, rendimiento, interoperabilidad, protección del medio ambiente, salud o seguridad, así como los requisitos aplicables al proveedor en lo que respecta a la información que debe facilitarse a la persona destinataria, tal como se especifica en el artículo 22, apartados 1 a 3, de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo de 12 de diciembre de 2006 relativa a los servicios en el mercado interior.

• los métodos y los criterios para evaluar el rendimiento de los productos de construcción, tal como se definen en el artículo 2, punto 1, del Reglamento (UE) n.º 305/2011

del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, por el que se establecen condiciones armonizadas para la comercialización de productos de construcción, en relación con sus características esenciales.

– Esquema Nacional de Interoperabilidad: Instrumento que comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

– Esquema Nacional de Seguridad: Instrumento que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

– Expediente administrativo: Conjunto ordenado de documentos y actuaciones relativos a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.

– Firma electrónica: Los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

– Firma electrónica avanzada: La firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento eIDAS.

– Firma electrónica cualificada: Una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

– Formato de documento: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria. Se corresponde habitualmente con una especificación técnica.

– Identificación: Procedimiento para reconocer de forma única la identidad de un sujeto que culmina tras un registro previo con la asignación de un elemento identificador singular en formato electrónico que representa de forma única a una persona física o jurídica o a una persona física que representa a una persona jurídica para interacción en el entorno digital.

– Infraestructura o servicio común: Capacidad organizativa y técnica que satisface necesidades comunes de las personas usuarias en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.

– Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

– Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos.

– Licenciamiento: Condiciones aplicables a la reutilización de cualquier tipo de material en formato electrónico que pueda ser empleado de forma recurrente.

– Marca de tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

– Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

– Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

– Nodo de interoperabilidad: Entidad que presta servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones Públicas bajo las condiciones que estas fijen.

– Política de firma electrónica: Conjunto de directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.

– Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

– Portal de internet de una Administración Pública: Se entiende por portal de internet el punto de acceso electrónico cuya titularidad corresponda a una Administración Pública, organismo público o entidad de derecho público que permite el acceso a través de internet a la información publicada y, en su caso, a la sede electrónica correspondiente.

– Prestador de Servicios de Confianza: Persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza, según lo previsto en el Reglamento eIDAS.

– Punto de Acceso General: Portal de internet que facilita el acceso a los servicios, trámites e información de los órganos, organismos públicos y entidades vinculados o dependientes de la Administración Pública correspondiente y aglutina o conduce a las sedes electrónicas asociadas de sus órganos y las sedes electrónicas de sus organismos públicos y entidades de derecho público.

– Sello electrónico: Datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.

– Sello electrónico avanzado: Sello electrónico que cumple los siguientes requisitos: 1) estar vinculado al creador del sello de manera única; 2) permitir la identificación del creador del sello; 3) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control, y 4) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.

– Sello electrónico cualificado: Sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico.

– Sede electrónica: Dirección electrónica, disponible para la ciudadanía a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de derecho público en el ejercicio de sus competencias.

– Sede electrónica asociada: Sede electrónica disponible para la ciudadanía a través de redes de telecomunicaciones que se crea por razones organizativas o técnicas vinculada a la sede electrónica de una Administración Pública o a la sede electrónica de un organismo público o entidad de derecho público.

– Sello de tiempo: Asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento

– Sistema de Interconexión de Registros: Infraestructura básica que permite el intercambio de asientos electrónicos de registro entre las Administraciones Públicas.

– Trazabilidad: Posibilidad de identificar el origen de un documento en las distintas fases de su producción, pudiendo determinar en qué fase y por quién se han producido, en su caso, las modificaciones del documento original.

# § 37

# Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas

Ministerio de la Presidencia
«BOE» núm. 245, de 9 de octubre de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-10264

El Consejo de Ministros, en su reunión de 19 de septiembre de 2014 y a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia y de los Ministros de Hacienda y Administraciones Públicas, del Interior, de Empleo y Seguridad Social y de Industria, Energía y Turismo, ha adoptado un Acuerdo por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.

En virtud de lo dispuesto en el apartado séptimo del citado Acuerdo y para general conocimiento, se dispone su publicación como Anexo a la presente Orden.

## ANEXO

### Acuerdo de Consejo de Ministros por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas

El Gobierno de España ha puesto en marcha un ambicioso proyecto reformista encaminado a corregir los desequilibrios que frenan nuestro crecimiento y crear las bases idóneas sobre las que levantar un nuevo ciclo de prosperidad económica y empleo.

Sobre estas premisas, el 26 de octubre de 2012 el Consejo de Ministros aprobó un Acuerdo por el que se crea la Comisión para la Reforma de las Administraciones Públicas (CORA) y tras la presentación de su Informe en el Consejo de Ministros de 21 de junio de 2013, se iniciaron actuaciones para simplificar los procedimientos y reducir las cargas administrativas para ciudadanos y empresas y para evitar solapamientos y duplicidades en las actuaciones de las Administraciones, propiciando la gestión de servicios y medios comunes con el objetivo de mejorar la eficacia de la actividad pública con ahorro de costes.

En el ámbito de los medios informáticos, las medidas propuestas por el Informe CORA se han centrado en una racionalización de las actuales estructuras organizativas en el ámbito de las Tecnologías de la Información y de las Comunicaciones (TIC) del Sector Público Administrativo Estatal, consolidando infraestructuras y servicios comunes que

permitan hacer una utilización más eficiente de los recursos tecnológicos, así como ofrecer mayores niveles de calidad en los servicios prestados.

Con el fin de desarrollar los procesos de estandarización que considera esenciales para incentivar la compartición y reutilización de las infraestructuras y servicios, el informe CORA contempló la creación de un órgano específico, al más alto nivel, que impulsara y coordinara el necesario proceso de racionalización de las diversas facetas de la política de tecnologías de la información y de comunicaciones en todo el ámbito del Sector Público Administrativo Estatal: adquisiciones de bienes informáticos, estructura de redes, servicios de administración electrónica y optimización de los sistemas de publicación web. Este órgano es la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado.

En desarrollo del informe CORA, las competencias para la coordinación del proceso de racionalización de las TIC en el Sector Público Administrativo Estatal se atribuyeron inicialmente al Ministerio de la Presidencia de acuerdo con lo dispuesto en el Real Decreto 695/2013, de 20 de septiembre. Este Real Decreto, atribuyó a la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado la elaboración, coordinación y dirección de la estrategia sobre tecnologías de la información y de las comunicaciones del Sector Público Administrativo Estatal, así como la planificación de la consolidación de las infraestructuras y servicios horizontales en el ámbito de la Administración Electrónica, entre otras. Por Real Decreto 802/2014, de 19 de septiembre, se atribuyen al Ministerio de Hacienda y Administraciones Públicas estas competencias y se adscribe a este Ministerio la Dirección de Tecnologías de la Información y las Comunicaciones dependiendo de la Secretaría de Estado de Administraciones Públicas.

En este modelo de gestión común e integrada, facilitadora de las relaciones entre sociedad y Administración, resulta esencial habilitar un sistema simple, rápido y seguro de identificación, autenticación y firma de los ciudadanos en su relación electrónica con los prestadores de servicios del Sector Público Administrativo Estatal y, en la medida que así se acuerde, del resto del Sector Público Estatal, de las Administraciones Autonómicas y Entidades Locales. Además, este sistema de identificación y autenticación electrónicas debe permitir la expresión de la voluntad del usuario, cuando así lo requiera el servicio o trámite electrónico, por medio de los sistemas de firma electrónica válidos según la normativa vigente.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, supuso que las Administraciones Públicas hicieran un enorme esfuerzo para poner todos sus servicios a disposición de la ciudadanía por medios electrónicos y hacerlo con las mayores garantías de seguridad posibles. Los altos niveles de seguridad previstos para el acceso electrónico a los servicios se han apoyado principalmente en los sistemas de firma electrónica previstos en los apartados a) y b) del artículo 13.2 de la Ley 11/2007 de 22 de junio. Estos sistemas de firma electrónica basada en certificados, requieren, sin embargo, actualizaciones de software y reconfiguraciones frecuentes que añaden un componente de complejidad que puede resultar disuasorio y que no es siempre necesario, en virtud del principio de proporcionalidad, en aquellos trámites y procedimientos que no requieran tan alto nivel de seguridad.

Por otra parte, aunque existen ya diferentes sistemas de identificación, autenticación y firma de los previstos en el artículo 13.2.c) de la Ley 11/2007, que prevé otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen, estos sistemas no son interoperables entre sí, con el trastorno que ello supone para el ciudadano al tener que conocer y aplicar distintos sistemas según la Administración, el organismo o el servicio o trámite al que acceda.

A la vista de estas dificultades, y en ejercicio de las funciones previstas en el artículo 9.1, apartado d) del Real Decreto 199/2012, de 23 de enero, que consisten en planificar la consolidación de las infraestructuras y servicios horizontales en el ámbito de la administración electrónica, el Ministerio de la Presidencia a través de la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado ha organizado y liderado los trabajos de un grupo de expertos en el que ha

participado representantes de la gran mayoría de los departamentos ministeriales y de sus organismos públicos adscritos, los cuales, tras un intenso trabajo de varios meses, han diseñado un sistema colaborativo de identificación, autenticación y firma electrónica, llamado a resolver las limitaciones de los actuales, integrando los sistemas de claves concertadas de la Administración ya existentes en uno único, y abriendo su utilización a la totalidad del Sector Público Administrativo Estatal, y permitiendo también integrarse al resto de las Administraciones Públicas cuando esté disponible, habilitando de este modo la extensión práctica de los servicios de Administración Electrónica a la gran mayoría de los ciudadanos españoles, en aplicación de la Ley 11/2007, de 22 de junio.

Por ello, atendiendo a las necesidades de los ciudadanos, aprovechando las posibilidades que la rápida evolución tecnológica ofrece y apelando al principio de proporcionalidad previsto en la Ley 11/2007, de 22 de junio, y sin perjuicio de la continuidad del servicio de los sistemas ya operativos, que resultan de indudable utilidad para los ciudadanos, se aprueba la creación de Cl@ve, un sistema común, de uso sencillo, basado en el artículo 13.2.c) de la citada ley que se conformará como la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas y ofrecerá servicios de identificación y autenticación alternativos y complementarios a los que se rigen por las letras a) y b) del artículo 13.2 de la Ley 11/2007, de 22 de junio. Este nuevo sistema pretende facilitar el acceso de los ciudadanos de forma uniforme a diversos servicios prestados vía Internet, tratando de minimizar los sistemas de identificación y autenticación existentes o aquellos que necesidades futuras pudieran demandar.

El sistema Cl@ve se desarrollará sobre dos sistemas ya operativos y, aprovechando el esfuerzo realizado en el seno del grupo de trabajo, se extiende el uso del PIN24H de la Agencia Estatal de Administración Tributaria, concebido para usuarios con acceso ocasional, y del «sistema de usuario y contraseña de la Seguridad Social» orientado a usuarios con acceso frecuente, recientemente implantados en sus respectivos ámbitos. Además, la transversalidad del nuevo modelo de gestión común de la identificación, autenticación y firma de los ciudadanos, al que se refiere el presente acuerdo, se fundamenta en la colaboración de los distintos órganos y organismos públicos adscritos a diversos departamentos ministeriales que actuarán en el sistema como órganos responsables de su aplicación y garantías de funcionamiento. Así, bajo la titularidad de la Dirección de Tecnologías de la Información y las Comunicaciones, que incorpora a las suyas las funciones hasta ahora atribuidas a la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, asumirán la responsabilidad de sus respectivas actuaciones en los ámbitos de Registro de usuarios, Identificación, Autenticación y Firma Electrónica la Agencia Estatal de Administración Tributaria, la Gerencia de Informática de la Seguridad Social y demás entidades Gestoras y Servicios Comunes de la Seguridad Social, la Dirección General de la Policía, como prestador de servicios de certificación, y a la FNMT-RCM, por la trascendencia que, en el desarrollo del proyecto, tiene el DNIe y la que en un futuro tendrá, sin duda, el DNI en la nube, ya que, adicionalmente, el sistema Cl@ve permitirá el acceso a servicios de firma en la nube basados en certificados electrónicos centralizados.

Este sistema de identificación y firma electrónica podrá evolucionar en el futuro para admitir también la participación del sector privado en su provisión, o su combinación con otras soluciones tecnológicas ofrecidas por empresas especializadas.

El sistema Cl@ve se crea para abarcar todo el ámbito del Sector Público Administrativo Estatal y, en su caso, del resto de las Administraciones Públicas. En este sentido cabe recordar que el impulso de una administración electrónica supone también dar respuesta a los compromisos comunitarios. La Agenda Digital para Europa propone medidas legales para el efectivo desarrollo digital de Europa en relación con la firma electrónica (acción clave n.º 3) y el reconocimiento mutuo de la identificación y la autenticación electrónicas (acción clave n.º 16), estableciendo así un marco jurídico claro con el fin de eliminar la fragmentación y la ausencia de interoperabilidad, potenciar la ciudadanía digital y prevenir la ciberdelincuencia.

En su desarrollo, la Ley 11/2007, de 22 de junio, consagra en su exposición de motivos el derecho de los ciudadanos a comunicarse con las Administraciones por medios electrónicos

e incide en que la contrapartida de este derecho es la obligación de las Administraciones de dotarse de los medios y sistemas electrónicos para que ese derecho pueda ejercerse de forma ágil y eficaz. La administración electrónica no es asunto meramente técnico, sino de gobernanza democrática y la extensión de una plataforma común a todas las instancias administrativas viene a satisfacer esa necesidad de homogeneidad, sencillez y servicios compartidos que recoge el informe CORA.

Siendo el ámbito de aplicación de este texto el conjunto del Sector Público Administrativo Estatal, y formando parte del mismo la Administración General del Estado, se adopta este Acuerdo de Consejo de Ministros en virtud de lo dispuesto en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, en su artículo 11 «Otros sistemas de firma electrónica»; dictado en desarrollo del artículo 13.2.c) de la Ley 11/2007, que indica que cuando el sistema se refiera a la totalidad de la Administración General del Estado, se requerirá acuerdo del Consejo de Ministros a propuesta de los Ministerios de la Presidencia y de Industria, Turismo y Comercio, previo informe del Consejo Superior de Administración Electrónica.

En virtud de lo expuesto, previo informe del Consejo Superior de Administración Electrónica y a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia, del Ministro de Hacienda y Administraciones Públicas, del Ministro del Interior, de la Ministra de Empleo y Seguridad Social y del Ministro de Industria, Energía y Turismo, el Consejo de Ministros en su reunión de 19 de septiembre de 2014, acuerda:

**Primero.** *Aprobación del sistema Cl@ve.*

Se aprueba el sistema Cl@ve, un sistema de identificación, autenticación y firma electrónica común para todo el Sector Público Administrativo Estatal, que permitirá al ciudadano relacionarse electrónicamente con los servicios públicos a través de una plataforma común mediante la utilización de claves concertadas previo registro como usuario de la misma, conforme a lo previsto en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Esta plataforma ofrecerá a los usuarios una interfaz amigable para seleccionar alguno de los sistemas de identificación y firma electrónica señalados en el artículo 13.2 de la Ley 11/2007, de 22 de junio.

La información relativa a este sistema, así como la relación de organismos del Sector Público Estatal, Administraciones Autonómicas o Entidades Locales que se incorporen al sistema, será publicada en el Portal www.060.gob.es y en las sedes electrónicas de los organismos en los que sea de aplicación de acuerdo con lo previsto en el Real Decreto 1671/2009, de 6 de noviembre por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio.

**Segundo.** *Órganos responsables de su aplicación y garantías de funcionamiento.*

1. El órgano responsable del sistema Cl@ve será la Dirección de Tecnologías de la Información y las Comunicaciones, en desarrollo de las competencias para el impulso de la Administración digital, y del proceso de innovación de la Administración General del Estado y sus Organismos Públicos. atribuidas de acuerdo con lo dispuesto en el Real Decreto 802/2014, de 19 de septiembre, por el que se modifican el Real Decreto 390/1998, de 13 de marzo, por el que se regulan las funciones y la estructura orgánica de las Delegaciones de Economía y Hacienda; el Real Decreto 1887/2011, de 30 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales; el Real Decreto 199/2012, de 23 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de la Presidencia; el Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas y el Real Decreto 696/2013, de 20 de septiembre, de modificación del anterior.

2. Participarán en la construcción e implantación del sistema Cl@ve y serán garantes de su funcionamiento, los siguientes órganos y organismos públicos, que asumirán la responsabilidad de sus respectivas actuaciones en los ámbitos de Registro de usuarios, Identificación, Autenticación y Firma Electrónica:

a) La Agencia Estatal de Administración Tributaria.

b) La Dirección de Tecnologías de la Información y las Comunicaciones.

c) La Gerencia de Informática de la Seguridad Social y demás entidades Gestoras y Servicios Comunes de la Seguridad Social

d) La Dirección General de la Policía

e) La Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM).

3. A los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado tendrá la condición de responsable del fichero, siendo los órganos y organismos públicos mencionados en el párrafo anterior encargados del tratamiento de la mismo, de acuerdo con su normativa específica. Por ello, y de conformidad con lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, dichos órganos y organismos públicos:

a) Tratarán los datos necesarios para el funcionamiento del sistema por cuenta del órgano responsable del fichero y conforme a las indicaciones que el mismo establezca, conforme al apartado quinto de este Acuerdo.

b) No tratarán los datos para fines distintos de los propios del sistema que consisten en facilitar al ciudadano una plataforma común que le permita relacionarse electrónicamente con los servicios públicos mediante la utilización de claves concertadas.

c) Implantarán, para el adecuado funcionamiento del sistema, las medidas de seguridad establecidas en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

d) Deberán, en caso, de cesar en la prestación del servicio, proceder a la devolución de los datos o a su transmisión al órgano u organismo que a tal efecto designase el responsable del fichero.

e) Respetarán, lo establecido en el artículo 12 de la Ley Orgánica 15/1999 y en el Capítulo III del Título II de su Reglamento de desarrollo.

4. El sistema permitirá varios modos de utilización, con diferentes niveles de garantía de funcionamiento con arreglo a criterios de integridad, confidencialidad, autenticidad y no repudio, en los términos previstos en el art. 11.3 del Real Decreto 1671/2009, de 6 de noviembre, que podrán ser aplicados a los procedimientos administrativos en función de sus necesidades, en virtud del principio de proporcionalidad recogido en el artículo 4 de la Ley 11/2007, de 22 de junio.

**Tercero.** *Descripción general del sistema Cl@ve.*

1. Registro:

Los interesados que deseen utilizar el sistema deberán facilitar los datos de carácter personal necesarios para habilitar los servicios de identificación, autenticación y firma electrónicas. Estos datos se integrarán en el Fichero Cl@ve de datos de carácter personal que se creará en los términos previstos en la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

El registro podrá realizarse de forma telemática o presencial en cualquiera de las oficinas de los órganos y organismos públicos que realicen funciones de Registro de usuarios de la plataforma Cl@ve. La forma de registro utilizada será uno de los factores para clasificar el nivel de garantía de identidad y autenticidad asociado al registro.

2. Identificación:

Existirán 2 tipos de sistemas de identificación:

a) Cl@ve ocasional: sistema de contraseña de validez muy limitada en el tiempo, orientado a usuarios que acceden esporádicamente a los servicios.

b) Cl@ve permanente: sistema de contraseña de validez duradera en el tiempo pero no ilimitada, orientado a usuarios habituales.

3. Firma de documentos electrónicos:

Los sistemas de Cl@ve podrán utilizarse para confirmar información, propuestas o borradores remitidos o exhibidos por una Administración Pública.

La plataforma Cl@ve ofrecerá a los usuarios una interfaz amigable que les permita seleccionar, de entre los sistemas de firma electrónica señalados en el artículo 13.2 de la Ley 11/2007, de 22 de junio, aquellos que exija o permita en cada caso la normativa reguladora de la actuación de que se trate para realizar el trámite o gestión administrativa correspondiente y la firma de documentos electrónicos en su caso.

Entre los sistemas ofrecidos al ciudadano, la plataforma Cl@ve ofrecerá al ciudadano utilizar el Documento Nacional de Identidad Electrónico para su identificación, autenticación y firma, en cuyo caso será aplicable al tratamiento de datos derivado de dicha utilización la normativa reguladora del citado documento.

**Cuarto.** *Aplicación del sistema.*

1. Cuando la realización de trámites o el acceso a servicios en una Sede Electrónica del Sector Público Administrativo Estatal requiera el uso de sistemas de identificación y autenticación de los previstos en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, deberá ofrecerse, como mínimo, alguno de los sistemas que se integren en la nueva plataforma Cl@ve.

2. Asimismo, con el fin de facilitar el acceso electrónico de los ciudadanos a la Administración y en desarrollo del principio de eficiencia, podrán adherirse al sistema mediante convenio otras Administraciones Públicas en las condiciones técnicas, económicas y organizativas que se determinen en las prescripciones técnicas de desarrollo a las que se refiere el apartado Quinto de este Acuerdo. Su incorporación al sistema Cl@ve será publicada en el Portal www.060.gob.es y en las sedes electrónicas que sean de aplicación.

3. Inicialmente funcionarán como Oficinas de Registro de datos la red de oficinas de la Agencia Estatal de Administración Tributaria y de las Entidades Gestoras y Servicios Comunes de la Seguridad Social. La Dirección de Tecnologías de la Información y las Comunicaciones de la Administración General del Estado podrá acordar ampliar la red de Oficinas de Registro con aquellos organismos públicos que dispongan de despliegue territorial y cumplan los requisitos técnicos necesarios establecidos por resolución de esta Dirección. La relación de Oficinas de Registro será publicada en el Portal www.060.gob.es y en las sedes electrónicas que sean de aplicación.

4. El Sector Público Administrativo Estatal deberá habilitar el sistema Cl@ve en todos los servicios y trámites electrónicos dirigidos a los ciudadanos antes del 31 de diciembre de 2015. Estarán excluidos los servicios y trámites dirigidos a ciudadanos que estén obligados por la normativa vigente al uso exclusivo de certificados electrónicos incluidos en el ámbito de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, así como el resto de trámites o servicios en los que la normativa reguladora no permita la utilización por los ciudadanos de los sistemas de identificación, autenticación y firma contemplados en la letra c) del artículo 13.2 de la Ley 11/2007, de 22 de junio.

**Quinto.** *Prescripciones técnicas.*

La Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado establecerá, mediante resolución, las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve, incluidos los siguientes aspectos:

1. Los elementos tecnológicos, procedimentales y organizativos necesarios para el desarrollo e implementación del sistema, y el aseguramiento de cada uno de los niveles de garantía de funcionamiento asociados a cada sistema de identificación de los previstos en este acuerdo.

2. Los procedimientos de registro de nuevos usuarios y los procedimientos para la incorporación de usuarios existentes en otros sistemas de firma ya operativos de los contemplados en el artículo 13.2 c) de la Ley 11/2007, de 22 de junio, previo consentimiento expreso de los mismos en los términos establecidos en la Ley 15/1999, de 13 de diciembre.

3. Las condiciones técnicas, económicas y organizativas para la incorporación de otras Administraciones Públicas al sistema Cl@ve.

4. El sistema de identificación e imputación de costes de mantenimiento y explotación del sistema Cl@ve correspondientes a órganos y organismos del Sector Publico Administrativo Estatal.

5. En general, todas las cuestiones necesarias para asegurar el funcionamiento de Cl@ve y su interoperabilidad.

**Sexto.** *No incremento del gasto público.*

La aplicación de las medidas previstas en el presente acuerdo se llevará a cabo sin incremento de gasto público.

**Séptimo.** *Efectos.*

El presente Acuerdo se publicará en el «Boletín Oficial del Estado», en el Portal www.060.gob.es y en las sedes electrónicas de los órganos y organismos de aplicación y producirá efectos desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

# § 38

## Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 311, de 29 de diciembre de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-14215

El Consejo de Ministros, en su reunión de 19 de septiembre de 2014 y, a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia y de los Ministros de Hacienda y Administraciones Públicas, del Interior, de Empleo y Seguridad Social y, de Industria, Energía y Turismo adoptó un Acuerdo por el que se aprueba Cl@ve, un sistema de identificación, autenticación y firma electrónica común para todo el Sector Público Administrativo Estatal que permitirá al ciudadano relacionarse electrónicamente con los servicios públicos a través de una plataforma común, mediante la utilización de claves concertadas previo registro como usuario de la misma, conforme a lo previsto en el artículo 13.2c) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

El citado Acuerdo publicado por Orden PRE/1838/2014, de 8 de octubre, determina en su apartado quinto, «Prescripciones Técnicas», que corresponde a la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado, establecer mediante resolución, las Prescripciones Técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve, y determina los aspectos que dichas prescripciones deben incluir.

En virtud de lo anterior, esta Dirección de Tecnologías de la Información y de las Comunicaciones resuelve:

**Primero.**

1. Aprobar las Prescripciones Técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve, en los términos recogidos en el Acuerdo de Consejo de Ministros de fecha de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas, que se incluyen como anexo.
2. Ordenar su publicación en el «Boletín Oficial del Estado».

**Segundo.**

La presente Resolución entra en vigor a partir del día siguiente a su publicación en el «Boletín Oficial del Estado».

# PRESCRIPCIONES TÉCNICAS NECESARIAS PARA EL DESARROLLO Y APLICACIÓN DEL SISTEMA CL@VE

## I. Objeto

Las presentes Prescripciones Técnicas tienen por objeto establecer los aspectos necesarios para el desarrollo y aplicación del sistema Cl@ve, así como para asegurar su funcionamiento e interoperabilidad.

## II. Ámbito de aplicación

Las presentes Prescripciones Técnicas serán de aplicación a:

a) Los órganos y organismos públicos participantes en la construcción e implantación del sistema Cl@ve y garantes de su funcionamiento.

b) Los órganos y organismos públicos del Sector Público Administrativo Estatal obligados a habilitar el sistema Cl@ve en todos los servicios y trámites electrónicos dirigidos a los ciudadanos.

c) Otras Administraciones Públicas que se adhieran al sistema.

d) Las entidades del sector privado que participen en el futuro como proveedores de sistemas de identificación y firma electrónica integrados con Cl@ve.

## III. Propósito del sistema Cl@ve

Cl@ve es un sistema de Identificación, Autenticación y Firma Electrónica común para todo el Sector Público Administrativo Estatal, basado en el uso de claves concertadas, conforme a lo previsto en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

El sistema Cl@ve está dirigido a ciudadanos españoles y extranjeros que cumplan los requisitos indicados en estas Prescripciones Técnicas y proporciona dos modalidades diferenciadas de identificación y autenticación basadas en el uso de claves concertadas para el acceso de los ciudadanos a los servicios electrónicos que hagan uso de este sistema, complementando los actuales sistemas de acceso mediante DNI-e y certificado electrónico reconocido.

Con este propósito, el sistema Cl@ve ofrecerá una interfaz amigable que permita al usuario seleccionar alguno de los sistemas de identificación y firma electrónica señalados en el artículo 13.2 de la Ley 11/2007, de 22 de junio.

Asimismo, el sistema Cl@ve permitirá al ciudadano el acceso al servicio de firma de documentos por medio de certificados electrónicos albergados tanto en modo local (por ejemplo en su PC) o en dispositivos conectados al mismo (por ejemplo, en el DNI-e) como en modo centralizado.

## IV. Niveles de garantía, sistemas de identificación, y firma de documentos electrónicos

### IV.1 Registro de usuarios.

Con objeto de garantizar un nivel adecuado de calidad en la identificación y autenticación que se llevan a cabo mediante el sistema Cl@ve, la utilización de dicho sistema requiere de un registro previo de los usuarios. Mediante dicho registro, se verifica la existencia de una persona física real asociada a la identidad electrónica que utilizará el sistema, se obtienen un conjunto de datos personales asociados a esa identidad, y se obtiene el consentimiento del usuario para que dichos datos personales sean incorporados al fichero de datos personales del sistema y sean tratados para la finalidad con la que se ha desarrollado el mismo.

Se podrán registrar en Cl@ve ciudadanos españoles con Documento Nacional de Identidad (DNI) y ciudadanos extranjeros con Tarjeta de Identidad de Extranjeros (TIE) o Certificado de Ciudadano de la Unión Europea; en ambos casos los documentos habrán de estar en vigor. La posibilidad de registro podrá ser extendida a ciudadanos españoles residentes en el extranjero sin DNI en vigor, mediante la habilitación de procedimientos de verificación de la identidad equivalentes a los establecidos para los ciudadanos con DNI.

Existirán dos modalidades o niveles de garantía de registro asociados a la forma y a las garantías que ofrezca la comunicación de la información de registro por parte del ciudadano:

a) Nivel Básico, en el que los datos del registro de usuario son facilitados por el ciudadano de forma telemática, pero sin una autenticación previa mediante certificado electrónico reconocido. La identificación se realizará utilizando datos conocidos por el ciudadano y la administración.

b) Nivel Avanzado, en el que los datos del registro de usuario son facilitados por el ciudadano, bien de forma presencial en una oficina ante un empleado público habilitado al efecto, o bien, son comunicados de forma telemática, previa autenticación del ciudadano mediante un certificado electrónico reconocido.

El nivel de garantía asociado al procedimiento de registro empleado quedará almacenado en el sistema Cl@ve, y podrá ser utilizado para seleccionar los modos de identificación válidos para cada procedimiento, en aplicación del principio de proporcionalidad previsto en el artículo 4 de la Ley 11/2007, de 22 de junio.

IV.2 Modalidades de identificación.

El sistema Cl@ve proporcionará a los usuarios dos modalidades de identificación electrónica basadas en el uso de claves concertadas, cada una de las cuales proporcionará dos niveles distintos de garantía en la autenticación:

c) Cl@ve ocasional o Cl@ve PIN: Modalidad de identificación para el acceso al sistema en el cual la contraseña, limitada a un solo uso, está formada por una clave aportada por el usuario más un código que recibe en su dispositivo móvil y que tiene una validez muy limitada en el tiempo. Está orientado a usuarios que acceden esporádicamente a los servicios.

El sistema de acceso basado en Cl@ve ocasional podrá ser denominado indistintamente Cl@ve PIN cuando sea mostrado a los usuarios del sistema para facilitar su identificación y acceso.

d) Cl@ve permanente: Modalidad de identificación para el acceso al sistema por medio de un identificador (Número de DNI o NIE del usuario) y una contraseña que debe ser custodiada por el ciudadano. La validez de la contraseña es duradera en el tiempo, pero no ilimitada. Adicionalmente, y cuando el tipo de trámite lo requiera, la modalidad de identificación Cl@ve permanente podrá proporcionar un nivel superior de garantía en la autenticación, para lo cual requerirá la utilización de una verificación de seguridad adicional mediante un código de un solo uso (OTP, «Once Time Password») y validez limitada en el tiempo enviado al dispositivo móvil del usuario. Está orientado principalmente para uso por parte de usuarios habituales.

Los requisitos de seguridad de las contraseñas para este sistema se publicarán en el portal Cl@ve (www.clave.gob.es)

El usuario podrá elegir en el momento de iniciar sesión en el Sistema Cl@ve qué modalidad de identificación prefiere utilizar, en función de las limitaciones establecidas por el proveedor de servicios electrónicos integrado con Cl@ve en cuanto a los niveles de garantía exigidos por el procedimiento o trámite al que se desea acceder.

IV.3 Firma de documentos electrónicos.

El sistema Cl@ve permitirá también el acceso a servicios de firma electrónica, en particular, a servicios de firma de documentos electrónicos mediante certificados electrónicos centralizados, todo ello a efecto de su presentación ante las Administraciones Públicas en aquellos trámites en que la firma mediante certificados electrónicos sea requerida o admitida. Se tendrán en cuenta las siguientes consideraciones:

a) Para poder acceder al servicio, el usuario deberá solicitar previa y expresamente la emisión de los certificados electrónicos centralizados correspondientes que posibilitan la firma mediante la plataforma Cl@ve.

b) Los certificados electrónicos centralizados serán emitidos con las mismas garantías de identificación del DNI electrónico del ciudadano

c) Para realizar la solicitud, y para el acceso ulterior al servicio, será necesario en todo caso que el usuario se haya registrado en Nivel Avanzado y haya activado su Cl@ve

permanente. Además se requerirá en el momento de la identificación la utilización de una verificación de seguridad adicional mediante un código de un solo uso y validez limitada en el tiempo que se enviará al teléfono móvil del usuario registrado.

A estos efectos, es de aplicación lo dispuesto en el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

IV.4 Punto de acceso al sistema Cl@ve.

Para facilitar el acceso a los servicios de identificación y autenticación del sistema Cl@ve, se creará un punto de acceso electrónico desde el que el ciudadano podrá identificarse de acuerdo a los diferentes niveles de garantía previstos en estas Prescripciones Técnicas. Con este propósito, el punto de acceso presentará un menú que permitirá al usuario elegir la modalidad de identificación electrónica deseada de entre las opciones puestas a disposición por el proveedor del servicio electrónico que soporta el tipo de trámite o procedimiento que desee realizar, de acuerdo con los niveles de garantía en el registro y la autenticación exigidos por dicho trámite o procedimiento.

El punto de acceso permitirá acceder a los servicios de identificación y autenticación previstos en el sistema Cl@ve, así como, en el futuro, a otros sistemas de identificación, entre ellos los sistemas de identificación electrónica de ámbito europeo admitidos en virtud de la normativa de la Unión Europea aplicable. Asimismo, el proveedor del servicio a efectos del cumplimiento del artículo 13 de la Ley 11/2007, podrá optar por habilitar sistemas de identificación no basados en claves concertadas complementarios al sistema Cl@ve, o por habilitar el acceso mediante el sistema Cl@ve a los medios de identificación previstos en el artículo 13.2, apartados a) y b) de la Ley 11/2007, opción que deberá incluir en todo caso los sistemas de firma electrónica incorporados al Documento Nacional de Identidad.

Las diversas Sedes Electrónicas de la Administración que requieran utilizar un sistema de identificación y autenticación de los previstos en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, deberán ofrecer, como mínimo, alguno de los sistemas de identificación mediante claves concertadas que se integren en la nueva plataforma Cl@ve.

Con este propósito, dichas Sedes Electrónicas deberán integrarse con el sistema Cl@ve actuando como proveedoras de servicios, redirigiendo automáticamente al ciudadano desde la sede electrónica al Punto de Acceso del sistema Cl@ve cuando el ciudadano desee realizar un trámite o procedimiento que precise algún sistema de identificación y autenticación de los previstos en el sistema Cl@ve. En esa redirección, las entidades deberán especificar el nivel de garantía en la autenticación que requiere el procedimiento o trámite al que desea acceder el ciudadano, pudiendo opcionalmente especificar también el nivel exigido de calidad en el registro. Una vez realizada la verificación de la identidad por parte de la entidad responsable de la modalidad de identificación seleccionada, el usuario será redirigido automáticamente al punto de origen, junto con el resultado de la autenticación, los datos que permiten identificar de manera no ambigua al ciudadano, y los niveles de garantías asociados a esa identidad.

Cuando el ciudadano se haya identificado y autenticado previamente en un servicio electrónico integrado con Cl@ve a través del Punto de Acceso, desde este Punto de Acceso se le dará la posibilidad de acceder a otro servicio electrónico sin necesidad de identificarse de nuevo, siempre que el proveedor de este segundo servicio lo permita. Esto supondrá que el ciudadano no tendrá que introducir los datos de identificación asociados a su Cl@ve PIN o Cl@ve Permanente.

Para asegurar esta integración con el Punto de Acceso del sistema Cl@ve, las entidades usuarias del sistema deberán seguir las especificaciones técnicas de integración definidas por las entidades responsables del mismo. Con el objeto de facilitar dicha integración, se habilitará un conjunto de componentes comunes, orientados a simplificar el manejo de los mensajes de petición y respuesta intercambiados durante el proceso de identificación y autenticación, que las entidades usuarias podrán incorporar a sus servicios electrónicos. Dichas especificaciones y componentes comunes se publicarán en el Centro de Transferencia de Tecnología.

La transmisión de información entre el Punto de Acceso del sistema Cl@ve y las sedes electrónicas integradas se protegerá de acuerdo con las mejores prácticas técnicas con

objeto de asegurar la privacidad, confidencialidad e integridad de dicha información. En este sentido, el Punto de Acceso del sistema Cl@ve no almacenará ningún dato de carácter personal, sino únicamente información técnica no vinculada a personas físicas o jurídicas, con el objeto de garantizar, en el caso de que se produzca un incidente, la reconstrucción, con la participación del proveedor del servicio electrónico al que accede el usuario y del proveedor del servicio de identificación de la modalidad de identificación escogida por este, de la secuencia de mensajes intercambiados entre los distintos actores del sistema para determinar el momento en que se produjo ese incidente y su naturaleza.

En el caso particular de los servicios electrónicos ofrecidos por los propios proveedores de servicios de verificación de la identidad de Cl@ve (AEAT y Seguridad Social, inicialmente), esta redirección al Punto de Acceso del sistema Cl@ve podrá ser sustituida por un acceso directo y equivalente a los servicios de verificación de la identidad de Cl@ve ofrecidos por dicho proveedor, siempre que el servicio electrónico no exija otro tipo de identificación diferente.

Adicionalmente, para facilitar el acceso a los servicios de firma electrónica con certificados electrónicos centralizados y presentar a los ciudadanos un mecanismo de firma uniforme en todo el sistema, se habilitará un conjunto de componentes de firma comunes que deberán ser integrados en las sedes electrónicas que requieran la realización de firma electrónica en sus trámites o procedimientos.

El Anexo I detalla los procedimientos de registro en el sistema Cl@ve, acceso al sistema Cl@ve y firma electrónica de documentos con certificados electrónicos centralizados asociados a los niveles de garantía del sistema Cl@ve previstos en estas Prescripciones Técnicas.

IV.5 Seguridad.

El sistema Cl@ve y todos los servicios asociados se implementarán garantizando su funcionamiento conforme a los principios de seguridad, integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 11/2007, de 22 de junio, en el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero y conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

V. Entidades encargadas del sistema, funciones y garantías aportadas por cada una

V.1 Registro de usuarios.

La Agencia Estatal de Administración Tributaria (AEAT) actuará como organismo principal responsable del sistema de Registro de usuarios de Cl@ve.

A tales efectos, este organismo será responsable del funcionamiento de los sistemas de registro de usuarios descritos en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito del registro de usuarios.

Inicialmente, con el fin de ofrecer un mejor servicio a los ciudadanos, estarán habilitadas y dispondrán de los medios necesarios para realizar funciones de registro de usuarios del sistema Cl@ve, además de la red de oficinas de la AEAT, las entidades gestoras de la Seguridad Social.

La Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) podrá acordar la adhesión al sistema de otros órganos y organismos del Sector Público Administrativo Estatal para actuar como oficina de registro de usuarios Cl@ve a fin de ofrecer a los ciudadanos nuevos puntos presenciales de registro, así como de órganos y organismos públicos pertenecientes a otras Administraciones.

En virtud de lo anterior, se ha habilitado para actuar como oficinas de registro presencial del sistema Cl@ve a la Red de oficinas de Información y Atención al Ciudadano de las Delegaciones y Subdelegaciones de Gobierno.

Los órganos y organismos distintos de la AEAT que actúen como oficinas de registro tendrán que cumplir los requisitos establecidos en la Resolución de 28 de septiembre de 2015 de la Dirección de Tecnologías de la Información y las Comunicaciones por la que se

establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve.

La DTIC mantendrá la relación de oficinas de registro de Cl@ve en el Punto de Acceso General http://administracion.gob.es.

V.2 Modalidad de identificación Cl@ve ocasional (Cl@ve PIN).

La AEAT actuará como organismo principal responsable del sistema de acceso basado en Cl@ve ocasional.

A tales efectos, la AEAT será la entidad encargada de realizar las funciones de identificación y autenticación de usuarios en esta modalidad de identificación, disponiendo de los medios necesarios para ello.

En consecuencia, la AEAT será responsable del funcionamiento del sistema de acceso basado en Cl@ve ocasional descrito en estas Prescripciones Técnicas así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito de la modalidad de identificación Cl@ve ocasional.

V.3 Modalidad de identificación Cl@ve permanente

La Gerencia de Informática de la Seguridad Social (GISS) actuará como organismo responsable del funcionamiento del sistema de acceso basado en Cl@ve permanente.

A tales efectos, la GISS será la entidad encargada de realizar las funciones de identificación y autenticación de usuarios en esta modalidad de identificación, disponiendo de los medios necesarios para ello, entre los que se cuenta una copia replicada del fichero de usuarios del sistema Cl@ve, necesario para verificar la identidad y las garantías de acceso.

En consecuencia, la GISS será responsable del funcionamiento del sistema de acceso basado en Cl@ve permanente descrito en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito de la modalidad de identificación Cl@ve permanente.

V.4 Emisión de certificados electrónicos centralizados para firma mediante la plataforma Cl@ve.

La entidad encargada de realizar las funciones de emisión y custodia de certificados electrónicos centralizados de usuarios para firma mediante la plataforma Cl@ve será, en el ejercicio de sus competencias, la Dirección General de la Policía (DGP), de acuerdo a la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad y al Real decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

Para realizar estas funciones, la DGP utilizará la Infraestructura de Clave Pública correspondiente al DNI electrónico actualmente existente.

La DGP, en el ejercicio de sus competencias, es responsable del funcionamiento del servicio de emisión y custodia de certificados electrónicos centralizados de usuarios, actuando como prestador de servicios de confianza de acuerdo con el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, y conforme a los principios de seguridad, integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 59/2003 de 19 de diciembre de Firma electrónica, y en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

V.5 Gestión de certificados electrónicos centralizados para firma mediante la plataforma Cl@ve.

La entidad encargada de realizar las funciones de almacenamiento y gestión de certificados electrónicos centralizados de usuarios para el sistema Cl@ve será la DGP.

Este organismo estará habilitado y dispondrá de los medios necesarios para realizar las funciones de almacenamiento y gestión de certificados descrita. Igualmente dispondrá de una copia replicada del fichero de certificados electrónicos indicado.

La GISS actuará como prestador de servicios de firma con certificado electrónico centralizado, para lo cual dispondrá de un respaldo de aquella información almacenada y

gestionada por la DGP necesaria para la firma. Dicha información estará sujeta a los siguientes requisitos:

a) la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;

b) el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.

La DGP es responsable del funcionamiento del servicio de almacenamiento y gestión de certificados descrito en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para este servicio.

V.6 Firma de documentos electrónicos mediante certificados electrónicos centralizados.

La entidad encargada de gestionar el entorno de creación de firma electrónica, en nombre del firmante, de documentos electrónicos mediante certificados electrónicos centralizados será la GISS que actuará como organismo responsable de este servicio, en unión con la DGP. A tales efectos, ambas entidades serán las habilitadas y dispondrán de los medios necesarios para realizar dichas funciones de firma de documentos electrónicos.

En consecuencia, ambos organismos serán los responsables del funcionamiento del servicio de firma de documentos electrónicos mediante certificados electrónicos centralizados descrito en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para este servicio.

V.7 Punto de acceso al sistema Cl@ve.

La entidad encargada de realizar las funciones correspondientes a la provisión del punto de acceso al sistema Cl@ve, de desarrollar los componentes comunes para facilitar la integración con este punto de acceso, y de desarrollar los componentes de firma comunes para el acceso al servicio de firma mediante certificados electrónicos centralizados será la DTIC.

La DTIC será responsable del funcionamiento del punto de acceso al sistema Cl@ve, de los componentes comunes para facilitar la integración con este punto de acceso y de los componentes de firma comunes para el acceso al servicio de firma mediante certificados electrónicos centralizados descritos en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito del punto de acceso y los componentes comunes de integración.

V.8 Garantía de alta disponibilidad.

Los organismos responsables del funcionamiento de los diferentes subsistemas que conforman Cl@ve establecerán un sistema de alta disponibilidad del servicio ofrecido.

V.9 Garantía de fiabilidad del entorno de creación de firma electrónica.

Los organismos responsables del funcionamiento de los diferentes subsistemas que conforman Cl@ve aplicarán procedimientos de seguridad específicos en materia de gestión y administración, y utilizarán sistemas y productos fiables, incluidos canales de comunicación electrónica seguros para garantizar que el entorno de creación de firmas electrónicas es fiable y se utiliza bajo el control exclusivo del firmante.

VI. Adhesión al sistema Cl@ve

El ámbito de aplicación del sistema Cl@ve podrá extenderse a otras Administraciones Públicas, mediante la formalización de un convenio al efecto con el Ministerio de Hacienda y Administraciones Públicas. En dicho convenio se establecerán las condiciones técnicas, económicas y organizativas de aplicación a otras Administraciones Públicas que complementarán, en su caso, a las establecidas en las presentes Prescripciones Técnicas.

VII. Sistema de identificación e imputación de costes

Con objeto de garantizar la sostenibilidad del sistema Cl@ve, se implementarán mecanismos para identificar y eventualmente imputar los costes de mantenimiento y

explotación del sistema a las diferentes entidades usuarias, basados en el uso efectivo del mismo por parte de dichas entidades.

Para ello, desde la DTIC se llevará un censo de las entidades integradas con el Punto de Acceso del sistema Cl@ve, de modo que únicamente las entidades incluidas en el censo puedan hacer uso del mismo. Cada petición de identificación y autenticación recibida por el Punto de Acceso se asociará a una entidad usuaria a través del identificador de entidad emisora que deberá incluirse en dichas peticiones, dejando una traza en el registro de actividad del sistema. Dichas trazas, que contendrán para cada petición la entidad emisora, el resultado y la modalidad de identificación utilizada, serán objeto de tratamiento para determinar el uso efectivo del sistema realizado por cada entidad y por consiguiente para realizar la imputación de costes.

Asimismo, para las funciones de firma de documentos electrónicos mediante certificados electrónicos centralizados, las entidades participantes en la provisión del servicio, GISS y DGP, implementarán un sistema de identificación e imputación de costes equivalente al anterior, basado en un censo de entidades integradas con el sistema de firma y un registro de actividad en el que se almacenarán las trazas de las peticiones de firma mediante certificados electrónicos centralizados recibidas.

## ANEXO I

### Procedimientos de registro, acceso al sistema y firma electrónica de documentos

Se describen a continuación los procedimientos inicialmente previstos en relación al registro de usuarios, así como de acceso al sistema y firma de documentos electrónicos. Estos procedimientos podrán ser adaptados de acuerdo a las necesidades y a la evolución del sistema Cl@ve para una mejor prestación del servicio a los ciudadanos.

La información actualizada de los procedimientos podrá encontrarse en www.clave.gob.es.

1. Procedimientos de alta en el registro.

Existirán tres procedimientos de registro diferenciados en el sistema Cl@ve: registro telemático sin certificado electrónico reconocido, registro telemático con DNI electrónico o certificado electrónico reconocido, y registro presencial.

1.1 Registro telemático sin certificado electrónico reconocido.

Esta modalidad de registro se corresponde con un Nivel de garantía de registro Básico.

Este procedimiento de registro se inicia mediante la solicitud por parte del ciudadano ante la entidad responsable del Registro, o a instancias de esta última sin solicitud previa, utilizando para esta identificación inicial del ciudadano un dato conocido por el ciudadano y la entidad. Una vez verificada la identidad, se remitirá a la dirección postal del ciudadano que conste en la entidad responsable del registro una carta de invitación al sistema Cl@ve, en la que se incluirá un código seguro de verificación (CSV).

Una vez recibida la carta, el ciudadano puede acceder a la aplicación de registro en Cl@ve, donde se le solicitan los datos personales necesarios para completar el registro, así como el código CSV de la comunicación emitida. Como medida de seguridad adicional en el momento del registro, también se solicitará un dato de verificación conocido por el ciudadano y la entidad.

Como respuesta, se emite un acuse de recibo firmado electrónicamente por el sistema con un CSV que incluye los datos proporcionados, y que incluirá el código de activación asociado al registro realizado.

1.2 Registro telemático con DNI electrónico o certificado electrónico reconocido.

Esta modalidad de registro se corresponde con un Nivel de garantía de registro Avanzado

Los ciudadanos con certificado electrónico reconocido o DNIe, podrán formalizar el registro en el sistema Cl@ve mediante una aplicación web sin necesidad de acudir a ninguna oficina.

El ciudadano accederá al punto de registro telemático de Cl@ve y se identificará con su certificado reconocido o DNIe. La aplicación de registro tomará del certificado los datos identificativos del ciudadano, y los verificará contra los que figuren en su DNI. Puesto que se tomarán como ciertos para su incorporación al registro los datos correspondientes al DNI, si los datos del DNI y del certificado no coinciden exactamente, se informará de esta discrepancia al ciudadano para que efectúe las correcciones pertinentes en la información proporcionada.

A continuación se le pedirán los otros datos necesarios para el registro, incluidos su número de teléfono móvil y su dirección de correo electrónico y firmará con su certificado esta solicitud, incluyendo la selección de la casilla donde declara haber leído y estar de acuerdo con los términos y condiciones de uso.

Se le dará un acuse de recibo firmado por el sistema con los datos proporcionados, documento que incluirá el código de activación asociado al registro realizado. El sistema informará al usuario de la utilidad del código de activación y se recalcará la importancia de su conservación para poderlo usar como factor de autenticación en caso de olvido de contraseña.

1.3 Registro presencial.

Esta modalidad de registro se corresponde con un Nivel de garantía de registro Avanzado

El ciudadano podrá registrarse en persona en cualquiera de las oficinas de registro autorizadas del sistema Cl@ve. Estas oficinas contarán con una aplicación de registro que les permitirá, una vez identificado el ciudadano ante un empleado público, formalizar el registro. Para asegurar el estricto control por parte del usuario de los medios de identificación utilizados en el sistema, no se permitirá que el registro presencial sea realizado por una persona en representación de otra.

El proceso de registro presencial se realizará de acuerdo con lo establecido en la Resolución de la Dirección de Tecnologías de la Información y las Comunicaciones por la que se establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve.

1.4 Bienvenida al sistema Cl@ve.

Una vez completado el registro en Cl@ve en cualquiera de las modalidades descritas anteriormente, el ciudadano recibirá, en el número de teléfono que acaba de registrar, un SMS de bienvenida al sistema.

A partir de la recepción de dicho SMS, el ciudadano registrado puede ya utilizar el sistema Cl@ve PIN y acceder a los sistemas de activación de contraseña del sistema Cl@ve permanente.

1.5 Obtención de nivel avanzado de garantía de registro.

Determinados servicios de Administración Electrónica requieren que el registro en Cl@ve se haya realizado con un nivel de garantía de registro avanzado, esto es, de forma presencial o telemáticamente con DNI electrónico o certificado electrónico reconocido.

Los ciudadanos que se hayan registrado en Cl@ve de forma telemática con una carta de invitación con un código seguro de verificación (CSV), y que por tanto dispongan únicamente de un nivel de garantía de registro básico, podrán solicitar la obtención del nivel avanzado personándose en las oficinas de registro o accediendo mediante DNIe o certificado electrónico reconocido a los sistemas de registro de Cl@ve.

1.6 Tratamiento del procedimiento de alta de un número de teléfono ya registrado.

El tratamiento descrito a continuación es común a los tres procedimientos de alta descritos anteriormente.

Por motivos de seguridad, el sistema requiere que un número de teléfono esté asignado a un único ciudadano usuario del sistema Cl@ve. En el caso de que un ciudadano intente registrarse con un teléfono que ya está dado de alta en el sistema asignado a otro usuario registrado, se seguirá este procedimiento para completar el registro:

1. Se explicará al ciudadano la situación detectada y se enviará un SMS con un código de un solo uso al número de teléfono móvil que se pretende registrar para que el usuario, o en su caso el empleado público que atiende el registro presencial, lo aporte en ese mismo momento para demostrar que el ciudadano es el poseedor del teléfono.

2. El sistema comprobará la validez del código de un solo uso aportado y en el caso de ser correcto se completará el registro y se procederá a revocar el número de teléfono al usuario que lo tenía anteriormente asignado. En caso contrario no se podrá completar el proceso de registro.

3. El usuario cuyo número de teléfono haya sido revocado en aplicación de este procedimiento no causará baja en el sistema Cl@ve, pero no podrá hacer un uso efectivo del mismo. Si el usuario intenta acceder al sistema se le informará que su usuario ha sido revocado por razones de seguridad con el fin de garantizar una asociación única con el número de teléfono móvil, y se le invitará a subsanar esta incidencia aportando un nuevo número de teléfono mediante el procedimiento establecido al efecto.

4. A los exclusivos efectos de informar al usuario que ha sido revocado su número de teléfono en aplicación de este procedimiento, el sistema podrá utilizar alguno de los datos de contacto incluidos en la Base de Datos de Registro para comunicarle esta incidencia y que pueda proceder a subsanarla, en su caso.

2. Procedimientos de baja en el registro.

Se habilitarán tres procedimientos de baja en el sistema Cl@ve:

2.1 Procedimiento de baja por renuncia.

El ciudadano puede renunciar a la utilización del sistema Cl@ve en cualquier momento, incluso aunque no se haya dado de alta en el mismo.

La renuncia podrá llevarse a cabo en el portal www.clave.gob.es, identificándose ante él y eligiendo en las opciones de usuario la de renuncia al sistema. En este caso el sistema deberá mostrar primero una pantalla de aviso para informar al usuario de que ya no podrá acceder al sistema y que si posteriormente quiere darse da alta deberá proceder de nuevo al procedimiento de registro como usuario. Si el ciudadano confirma esta pantalla, el sistema marcará al usuario como dado de baja por renuncia. Indistintamente podrá realizar esta petición usando DNIe o certificado electrónico reconocido o de manera presencial en una oficina. Si el registro se ha realizado a nivel básico, mediante carta de invitación, la renuncia también se podrá tramitar mediante el código CSV incluido en la misma.

Si un ciudadano renuncia al sistema, se revocará su certificado electrónico centralizado, caso de existir, y se deshabilitará su acceso electrónico tanto mediante Cl@ve PIN como mediante Cl@ve Permanente a los servicios de identificación, autenticación y firma electrónica Cl@ve.

2.2 Procedimiento de revocación de oficio.

El sistema Cl@ve podrá gestionar la revocación de oficio de usuarios registrados en el sistema cuando concurran circunstancias que pongan en riesgo la seguridad del mismo, como un uso fraudulento o desleal del sistema o cuando se produzca una modificación sustancial de los datos de identificación utilizados en el registro, como son el cambio del nombre o los apellidos en su DNI o la nacionalización o expulsión de extranjeros.

A los exclusivos efectos de informar al usuario que ha sido revocado en aplicación de este procedimiento, el sistema podrá utilizar alguno de los datos de contacto incluidos en la Base de Datos de Registro para comunicarle esta incidencia.

La revocación solo podrá dar lugar a una nueva alta cuando se hayan modificado las circunstancias que motivaron la misma.

Los efectos de la revocación serán los mismos que los de la renuncia, de forma que se revocará su certificado electrónico centralizado, caso de existir, y se deshabilitará su acceso electrónico tanto mediante Cl@ve PIN como mediante Cl@ve Permanente a los servicios de identificación, autenticación y firma electrónica de Cl@ve.

2.3 Procedimiento de baja por fallecimiento.

El sistema Cl@ve gestionará automáticamente y de oficio la baja de los usuarios fallecidos de los que se tenga constancia y se encuentren registrados. Los efectos de la baja

por fallecimiento serán los mismos que los de la renuncia: se revocará el certificado electrónico centralizado del usuario, caso de existir, y se deshabilitará su acceso electrónico tanto mediante Cl@ve PIN como mediante Cl@ve Permanente a los servicios de identificación, autenticación y firma electrónica de Cl@ve.

3. Procedimientos de modificación de datos en el registro.

Se habilitarán los siguientes procedimientos de modificación de datos del registro:

3.1 Procedimiento de modificación del número de móvil.

Si el ciudadano desea modificar el número de móvil que notificó durante el acto del registro, deberá acudir de nuevo a una oficina de registro donde le actualizarán, previa identificación con su DNI, TIE o Certificado de Ciudadano de la Unión Europea, el número de teléfono móvil en la base de datos y le proporcionarán un nuevo código de registro para futuras operaciones, teniendo que firmar de nuevo el correspondiente documento de aceptación. También podrá hacer la operación de forma telemática, si el usuario dispone de un certificado electrónico reconocido o DNIe.

En el caso de que el nuevo número de teléfono móvil ya esté dado de alta en el sistema, se aplicará el procedimiento de alta de un número de móvil ya registrado descrito anteriormente.

El procedimiento de modificación del número de móvil no implica la revocación del certificado electrónico centralizado del ciudadano ni la desactivación de su usuario y contraseña de acceso.

3.2 Procedimiento de modificación de otros datos.

El usuario registrado en el sistema puede modificar otros datos asociados al registro, a excepción del número de DNI y del nombre y los apellidos.

Estas modificaciones se podrán realizar telemáticamente en el portal www.clave.gob.es o en una de las oficinas de registro.

El procedimiento de modificación de estos datos no generará un nuevo código de activación aunque sí el documento de aceptación de condiciones, donde se incluirán los nuevos datos declarados por el ciudadano.

4. Procedimiento de uso de Cl@ve PIN.

En la Modalidad de Identificación Cl@ve ocasional, el usuario aportará la primera parte de su clave y recibirá un código en su dispositivo móvil, de validez muy limitada en el tiempo, que conjuntamente conforman el código de acceso.

Para reforzar la seguridad del sistema de identificación y autenticación se divide el código de acceso (Cl@ve PIN) en dos partes:

• Clave de acceso: la define el usuario cada vez que solicita un Cl@ve PIN. No tiene que ser siempre la misma.
• PIN: la envía el sistema Cl@ve al móvil del usuario cuando lo solicita.

De manera que la unión de ambos datos conforma el Código de Acceso.

Código de Acceso (Cl@ve PIN) = Clave de Acceso + PIN.

Este sistema permite al ciudadano tener el control sobre una parte del código de acceso de forma que es el usuario quien lo define cada vez que solicita un PIN. Como medida de seguridad adicional, este código nunca se envía en claro al sistema Cl@ve. De esta manera, se logra que, aunque otra persona pudiera tener acceso a estos mensajes, no podría suplantar al usuario pues le faltaría conocer la parte del código que define el propio usuario.

Se definen los siguientes procedimientos relativos a la obtención y utilización del sistema Cl@ve PIN:

4.1 Procedimiento de obtención de Cl@ve PIN.

Para la obtención de un PIN en el sistema Cl@ve, el solicitante deberá acceder al portal de gestión de la Cl@ve ocasional, donde deberá introducir su usuario Cl@ve (número del DNI o NIE), información de contraste conocida por ambas partes, elegir una clave de acceso, que no es necesario que sea siempre la misma, y solicitar un nuevo PIN. Como resultado, el

sistema Cl@ve enviará un código al teléfono móvil registrado con el que el usuario podrá completar la autenticación.

4.2 Procedimiento de utilización de Cl@ve PIN.

Para completar la autenticación en el sistema el usuario deberá introducir su usuario Cl@ve (DNI o NIE) y su código de acceso formado por la clave seleccionada en el momento de la obtención y el PIN recibido en su teléfono móvil.

Si el solicitante introduce erróneamente el código de acceso más veces de las permitidas, por motivos de seguridad, se bloqueará el acceso de forma temporal.

La validez del PIN es la siguiente:

• Validez temporal: Se deberá utilizar el PIN que se ha recibido en el teléfono móvil para completar el acceso al sistema antes de 10 minutos. Pasado ese tiempo, si no se ha llegado a acceder a Cl@ve, se deberá solicitar un nuevo PIN.

• Número de usos: El PIN se configura como una clave de un solo uso (OTP), de forma que se garantice que siempre que se solicite una autenticación con Cl@ve PIN se fuerce al usuario a iniciar el proceso de solicitud de un nuevo PIN para poder autenticarse en esa sesión.

• Sesión: Una vez identificado mediante Cl@ve PIN se puede acceder a los servicios que permitan Cl@ve hasta que se produzca la desconexión de la Sede Electrónica o se cierre el navegador.

5. Procedimientos de activación y gestión de contraseñas.

Se definen los siguientes procedimientos relativos a la activación de cuentas de usuario en el sistema Cl@ve y gestión de las contraseñas:

5.1 Procedimiento de activación.

Para la activación de la cuenta de usuario en el sistema Cl@ve, necesaria para poder utilizar la modalidad de identificación de Cl@ve permanente, el solicitante deberá acceder al portal www.clave.gob.es, donde deberá introducir su identificador de usuario Cl@ve (DNI o NIE), su dirección de correo electrónico y el código de activación que se le ha suministrado en el acto del registro. Si son correctos, el sistema le enviará un mensaje al móvil con un código de un solo uso que el usuario deberá introducir en el sistema y, una vez comprobado, le permitirá introducir la contraseña que prefiera para acceder ulteriormente a Cl@ve, cumpliendo con las características mínimas de seguridad definidas.

Si el solicitante introduce erróneamente el código de activación más veces de las permitidas, el código de activación quedará bloqueado por motivos de seguridad y se precisará la generación de uno nuevo.

5.2 Procedimiento de cambio de contraseña.

Las contraseñas de los usuarios caducarán en el plazo determinado por la política de seguridad del sistema, plazo que se comunicará en el portal www.clave.gob.es. En cualquier caso, el usuario podrá cambiar la contraseña de acceso en cualquier momento. Para ello accederá al sistema con su usuario y contraseña y dentro de las opciones de usuario elegirá cambiar contraseña. Introducirá la nueva contraseña y el sistema le enviará un código de un solo uso al móvil para confirmar la operación.

Esta operación podrá realizarse también accediendo con DNIe o certificado reconocido, en cuyo caso no hará falta el código de un solo uso.

5.3 Procedimiento de restablecimiento de contraseña.

Este procedimiento será necesario si el ciudadano olvida su contraseña o ésta queda bloqueada al producirse el número máximo de intentos fallidos en la introducción de la misma. En tal caso habrá de establecerse una contraseña nueva.

Para restablecer la contraseña, el ciudadano accederá al sistema con su usuario y seleccionará la opción de «restablecimiento de contraseña». El sistema le pedirá el código de activación que se le entregó en el proceso de registro y que deberá coincidir con el que consta en la base de datos. Si es correcto, el sistema enviará un código de seguridad al móvil del ciudadano, código que deberá introducir para restablecer la contraseña.

5.4 Procedimiento de recuperación del código de activación.

Si el usuario desea restablecer la contraseña y no dispone del código de activación, podrá obtener un nuevo código de activación acudiendo a una oficina de registro o telemáticamente autenticándose mediante certificado electrónico reconocido o DNIe o mediante Cl@ve PIN. Esta operación no precisa la emisión del documento de aceptación puesto que el ciudadano no está declarando ningún dato nuevo.

6. Procedimientos de gestión de certificados y firma electrónica.

Los siguientes procedimientos son de aplicación en relación a los certificados electrónicos centralizados para firma.

6.1 Procedimiento de emisión de los certificados centralizados para firma con la plataforma Cl@ve.

Una vez que el usuario se ha registrado en el sistema con nivel avanzado de garantía de registro, ha activado su Cl@ve Permanente, y ha solicitado expresamente la emisión de sus certificados electrónicos centralizados para firma mediante la plataforma Cl@ve, dicha emisión se llevará a cabo la primera vez que el ciudadano acceda al procedimiento de firma con el sistema Cl@ve.

El sistema informará al ciudadano de que se le va a emitir su certificado, así como de las garantías de seguridad ofrecidas por la Administración para la custodia y acceso al mismo, y generará en ese momento su clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice, con un alto nivel de confianza, su uso bajo el control exclusivo de su titular.

La generación de los certificados deberá hacerse acorde con los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el ciudadano realizó el registro presencial.

6.2 Procedimiento de firma con certificado electrónico centralizado.

El procedimiento de firma electrónica con certificado electrónico centralizado garantizará que el acceso a los datos de creación de firma asociados al certificado sólo sea efectuado por el titular del mismo, por lo que para su uso se deberá haber autenticado previamente al ciudadano mediante dos factores de autenticación: la pareja identificador de Cl@ve con su contraseña de Cl@ve permanente, y un código de un solo uso (OTP) enviado por SMS a su móvil.

6.3 Procedimiento de renovación de los certificados electrónicos centralizados.

La renovación de los certificados centralizados para firma mediante la plataforma Cl@ve se podrá llevar a cabo de forma automática siempre y cuando se cumplan los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el ciudadano realizó el registro presencial. En caso contrario, para renovar su certificado el ciudadano tendrá que personarse en una oficina de registro para que se le provea de un nuevo código de activación y pueda volver a activarse su usuario y sus certificados.

La renovación automática se producirá cuando el ciudadano se disponga a firmar, se haya autenticado para poder acceder a su clave de firma y se detecte en ese momento que su certificado está caducado o próximo a caducar, hasta 2 meses antes de la fecha de expiración de su validez. En ese caso el sistema Cl@ve emitirá y almacenará automáticamente los nuevos certificados revocando previamente los antiguos, de acuerdo a la normativa vigente sobre certificados electrónicos reconocidos.

En todo caso el sistema informará al ciudadano de que se ha procedido a la renovación automática de sus certificados y le comunicará el nuevo periodo de validez de los mismos, informando también de que los anteriores certificados han sido revocados, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

6.4 Procedimiento de revocación.

La revocación de los certificados electrónicos centralizados del ciudadano se llevará a efecto en caso de renuncia o baja voluntaria del ciudadano en el sistema, en el caso de baja

por fallecimiento y en el caso de revocación de oficio del acceso al sistema llevada a cabo por la Administración en las circunstancias que se determinen.

Una vez revocado un certificado, el sistema garantizará que no se podrá utilizar a partir de ese momento durante un proceso de firma.

El sistema podrá permitir también, con las garantías que se consideren necesarias, que el propio ciudadano pueda solicitar tanto presencial como telemáticamente la revocación exclusiva de su certificado electrónico de firma centralizado, sin necesidad de darse de baja en el sistema Cl@ve. La revocación deberá constatarse documentalmente, por lo que en cualquiera de estos procedimientos el ciudadano deberá firmar la solicitud de renuncia o revocación, ya sea con un certificado electrónico reconocido o de forma manuscrita.

7. Procedimientos de incorporación de registros de otros censos.

Tal y como establece el Acuerdo del Consejo de Ministros de creación de Cl@ve, para incorporar al Censo Cl@ve usuarios registrados en otros sistemas de identificación, autenticación y firma que existan con anterioridad al propio acuerdo, se deberá solicitar el consentimiento expreso del ciudadano.

En cualquier caso, los procedimientos de incorporación asegurarán que en estos censos se han cumplido los requisitos necesarios para poder asignar el nivel de garantía de registro y el sistema de identificación y autenticación correspondientes en el sistema Cl@ve. Asimismo, el procedimiento deberá permitir comprobar la veracidad y exactitud de los datos aportados desde los otros censos y se solicitará al usuario la aportación de los datos complementarios necesarios para completar el registro, todo ello manteniendo las mismas garantías que aplican al procedimiento de alta de usuarios en el sistema Cl@ve.

Se integrarán en una primera fase los censos del sistema PIN24H de la AEAT y del sistema usuario-contraseña de la Seguridad Social. En cualquier caso, la incorporación de registros de otros censos requerirá la autorización de la DTIC.

# § 39

## Orden PCM/1382/2021, de 9 de diciembre, por la que se regula el Registro Electrónico General en el ámbito de la Administración General del Estado

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 296, de 11 de diciembre de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-20477

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, actualmente derogada, ya establecía en el artículo 24 que las Administraciones Públicas crearían registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones. Posteriormente, el Real Decreto 1671/2009, de 6 de noviembre, que desarrolló parcialmente esta ley, preveía la creación del Registro Electrónico Común de la Administración General del Estado que finalmente sería desarrollado por la Orden HAP/566/2013, de 8 de abril.

El artículo 16 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establece que cada Administración dispondrá de un Registro Electrónico General en el que se hará el correspondiente asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, organismo público o entidad, vinculados o dependientes. También se podrá anotar la salida de los documentos oficiales dirigidos a otros órganos o particulares.

El precepto establece que los organismos públicos vinculados o dependientes de cada Administración podrán disponer de su propio registro electrónico plenamente interoperable e interconectado con el Registro Electrónico General de la Administración de la que depende.

Estos registros electrónicos contarán con el apoyo de las Oficinas de Asistencia en Materia de Registros a las que corresponde la digitalización y la anotación en el Registro Electrónico General, o registro electrónico de cada organismo o entidad según corresponda, de las solicitudes, escritos y comunicaciones en papel que se presenten o sean recibidos en estas y se dirijan a cualquier órgano, organismo público o entidad de derecho público de cualquier Administración Pública.

Para dar cumplimiento a estas previsiones legales, el artículo 38 del Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, establece la naturaleza y funcionamiento del Registro Electrónico General de la Administración General del Estado.

De acuerdo con lo señalado anteriormente, se considera necesario regular los requisitos y condiciones del funcionamiento del Registro Electrónico General de la Administración General del Estado.

Esta orden se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En este sentido, la norma da cumplimiento a los principios de

necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia. La misma persigue un interés general al pretender incrementar la eficiencia y la transparencia en el funcionamiento del sector público estatal. No existe ninguna alternativa regulatoria menos restrictiva, resulta coherente con el ordenamiento jurídico, no introduce nuevas cargas administrativas, y permite una gestión más eficiente de los recursos públicos.

Esta orden ha sido informada por la Agencia Española de Protección de Datos, en virtud del artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y del artículo 5.3 b) del Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio.

En su virtud, a propuesta conjunta de la Vicepresidenta Primera del Gobierno y Ministra de Asuntos Económicos y Transformación Digital y de la Ministra de Hacienda y Función Pública, dispongo:

**Artículo 1.** *Objeto y ámbito de aplicación.*

1. La orden tiene por objeto regular los requisitos y condiciones del funcionamiento del Registro Electrónico General de la Administración General del Estado, (en adelante, REG-AGE).

2. De acuerdo con el artículo 38 del Reglamento de actuación y funcionamiento del Sector Publico por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, el REG-AGE se configura como el conjunto agregado de los asientos practicados a través de las aplicaciones de que dispongan las unidades que realicen anotaciones en registro, de las anotaciones que se realicen en cualquier aplicación que proporcione soporte a procedimientos específicos, así como de las anotaciones que se practiquen por medio del servicio electrónico para la presentación de solicitudes, escritos y comunicaciones accesible desde la sede electrónica del Punto de Acceso General de la Administración General del Estado.

3. El ámbito del REG-AGE es la Administración General del Estado y sus Organismos públicos y Entidades de derecho público vinculados o dependientes que no dispongan de su propio registro.

**Artículo 2.** *Órganos competentes.*

1. La Dirección General de Gobernanza Pública del Ministerio de Hacienda y Función Pública es competente para la gobernanza y gestión funcional del REG-AGE, correspondiendo a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital el diseño, implantación y gestión técnica de la plataforma tecnológica del REG-AGE y del servicio electrónico para la presentación de solicitudes, escritos y comunicaciones accesible desde la sede electrónica del Punto de Acceso General de la Administración General del Estado.

2. En cada Ministerio se designará una persona delegada del REG-AGE, con rango de Subdirector General o asimilado, pudiendo nombrar más de una persona delegada cuando el volumen de actividad o número de Oficinas de Asistencia en Materia de Registros así lo aconseje. La designación corresponderá al titular de la Subsecretaría o en su caso al Presidente o Director de sus organismos públicos y entidades de derecho público vinculados o dependientes.

La persona delegada será responsable del seguimiento del correcto funcionamiento del REG-AGE sobre los documentos que tengan como emisor o destinatario el ministerio y los organismos públicos y entidades de derecho público vinculados o dependientes y la coordinación de las Oficinas de Asistencia en Materia de Registros en relación con el REG-AGE.

**Artículo 3.** *Acceso al Registro Electrónico General de la Administración General del Estado.*

1. De acuerdo con lo previsto en el artículo 16 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se podrá acceder al REG-AGE a través de las siguientes vías:

a) Presencialmente, exclusivamente para los sujetos no obligados a relacionarse electrónicamente de acuerdo con el artículo 14 de la ley 39/2015, de 1 de octubre, a través de las Oficinas de Asistencia en Materia de Registros y en las representaciones diplomáticas u oficinas consulares de España en el extranjero. Asimismo, en las oficinas de Correos en los términos que se determinen reglamentariamente.

b) Por internet, a través de la sede electrónica del Punto de Acceso General de la Administración General del Estado (sede.administracion.gob.es) que dispondrá de un acceso al REG-AGE para la presentación de solicitudes, escritos y comunicaciones distintos de los mencionados en el apartado c).

c) Por internet, a través de las sedes electrónicas asociadas a los ministerios, organismos y entidades de derecho público de la Administración General del Estado para los servicios, procedimientos y aplicaciones de soporte que realicen anotaciones en el REG-AGE.

2. El Punto de Acceso General de la Administración General del Estado o su sede electrónica contendrá:

a) Información sobre las distintas vías de acceso al REG-AGE señaladas en el apartado 1.

b) Un enlace al servicio del REG-AGE accesible desde la sede electrónica del Punto de Acceso General de acuerdo con el apartado 1.b), junto con la descripción de los requisitos técnicos del servicio, el detalle del formulario general a utilizar para la presentación de solicitudes, escritos y comunicaciones y las especificaciones de la documentación que, en su caso, se acompañe.

c) Información actualizada de los servicios, procedimientos y trámites que cuenten con aplicaciones específicas que realicen anotaciones en el REG-AGE y un enlace a las sedes electrónicas a través de las cuales se acceda a los mismos.

**Artículo 4.** *Anotación en el Registro Electrónico General de la Administración General del Estado.*

1. Los asientos registrales en el REG-AGE se anotarán respetando el orden temporal de recepción o salida de los documentos, e indicarán la fecha y hora del día en que se produzcan. Concluido el trámite de registro en el REG-AGE, los documentos serán cursados sin dilación a sus destinatarios y a las unidades administrativas correspondientes desde el registro en que hubieran sido recibidas.

Los datos, formatos y protocolos así como la documentación para integradores se detallan en el Portal de la Administración Electrónica (PAe) en el siguiente enlace: https://administracionelectronica.gob.es/.

2. Se garantizará la constancia, en cada asiento que se practique, de un número, epígrafe expresivo de su naturaleza, fecha y hora de su presentación, identificación de la persona interesada, órgano administrativo remitente, si procede, y persona u órgano administrativo al que se envía, y, en su caso, referencia al contenido del documento que se registra.

**Artículo 5.** *Documentos admisibles a través del servicio electrónico accesible desde la sede electrónica del Punto de Acceso General.*

1. El servicio electrónico para la presentación de solicitudes, escritos y comunicaciones accesible a través de la sede electrónica del Punto de Acceso General de la Administración General del Estado admitirá cualquier solicitud, escrito o comunicación relacionado con servicios, procedimientos y trámites que no cuenten con aplicaciones de soporte que realicen anotaciones en el REG-AGE.

2. El formulario general a utilizar para la presentación de solicitudes, escritos y comunicaciones a través de este acceso estará disponible en la propia sede electrónica del Punto de Acceso General de la Administración General del Estado.

3. Si fuera precisa la aportación de documentación complementaria que supere la extensión máxima a presentar en un solo registro electrónico se podrá llevar a cabo mediante una nueva presentación que incluirá, al menos, la referencia al número o código de

registro individualizado al que complementa o información suficiente que permita identificarlo.

**Artículo 6.** *Acuse de recibo.*

1. Independientemente del sistema de acceso al REG-AGE, se emitirá, automáticamente, un recibo firmado electrónicamente mediante alguno de los sistemas de firma previstos en el artículo 40 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con el siguiente contenido:

a) El número o código de registro individualizado.
b) La fecha y hora de presentación.
c) La copia autenticada del escrito, comunicación o solicitud presentada, siendo admisible a estos efectos la reproducción literal de los datos introducidos en el formulario de presentación.
d) En su caso, la enumeración y denominación de los documentos adjuntos al formulario de presentación o documento presentado, seguida de la huella electrónica de cada uno de ellos.

2. El citado recibo electrónico tendrá la consideración de acuse de recibo y su emisión no prejuzga la admisión definitiva del escrito de acuerdo con lo previsto en el artículo 16.8 de la Ley 39/2015, de 1 de octubre.

**Artículo 7.** *Consultas al REG-AGE.*

Desde el servicio electrónico de registro accesible desde la sede electrónica del Punto de Acceso General, el interesado podrá consultar sus asientos registrales realizados en el REG-AGE mediante dicho servicio, que contendrá, al menos:

a) El estado de las presentaciones.
b) El recibo de los asientos registrales.
c) Los documentos adjuntos correspondientes al asiento registral.

**Artículo 8.** *Presentación de documentos, fecha, hora oficial y cómputo de plazos.*

1. Cuando se acceda por internet al REG-AGE se permitirá la presentación de solicitudes, escritos y comunicaciones todos los días del año, durante las 24 horas del día, sin perjuicio de las interrupciones de mantenimiento técnico u operativo, que se anunciarán con la antelación que resulte posible y, en todo caso, con un mínimo de 24 horas en la sede electrónica del Punto de Acceso General de la Administración General del Estado junto con la ampliación concreta del plazo no vencido, según el artículo 32.4 de la Ley 39/2015, de 1 de octubre.

Cuando, por tratarse de interrupciones no planificadas que impidan la presentación de escritos, no resulte posible realizar su anuncio con antelación, se actuará conforme a lo establecido en el artículo 32.4 de la Ley 39/2015, de 1 de octubre, a cuyo efecto se podrá determinar una ampliación de los plazos no vencidos, debiendo publicarse en la sede electrónica tanto la incidencia técnica acontecida como la ampliación concreta del plazo no vencido.

Conforme a lo establecido en el artículo 31.2 de la Ley 39/2015, de 1 de octubre, la fecha y hora a computar en las anotaciones del REG-AGE será la oficial de la sede electrónica del Punto de Acceso General de la Administración General del Estado, debiendo adoptarse las medidas precisas para asegurar su integridad.

2. Para la presentación por internet a través de las sedes electrónicas asociadas de los ministerios, o las sedes electrónicas asociadas de los organismos públicos y entidades de derecho público de la Administración General del Estado para los servicios, procedimientos y trámites que cuenten con modelos normalizados de presentación y aplicaciones de soporte que realicen anotaciones en el REG-AGE, la fecha y hora a computar será la oficial de la correspondiente sede electrónica.

3. Para la presentación de documentos en las Oficinas de Asistencia en Materia de Registros se publicará en el Punto de Acceso General el listado de las oficinas y los días y el horario en el que permanecen abiertas.

4. El calendario de días inhábiles a efectos de cómputo de plazos en el REG-AGE será el que se determine en la resolución publicada cada año en el «Boletín Oficial del Estado» para todo el territorio nacional por el Ministerio de Hacienda y Función Pública, en cumplimiento del artículo 30.7 de la Ley 39/2015, de 1 de octubre.

**Artículo 9.** *Responsabilidad.*

Los usuarios asumen con carácter exclusivo la responsabilidad de la custodia de los elementos necesarios para su identificación en el acceso a los servicios prestados mediante administración electrónica, el establecimiento de la conexión precisa y la utilización de la firma electrónica, así como de las consecuencias que pudieran derivarse del uso indebido, incorrecto o negligente de los mismos.

Los departamentos ministeriales, entidades y organismos públicos destinatarios de los escritos presentados en el REG-AGE serán responsables de la custodia y manejo de los correspondientes ficheros, una vez se haya producido su entrega y recepción.

**Artículo 10.** *Protección de datos de carácter personal.*

De conformidad con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando la persona interesada o su representante fueran personas físicas, el tratamiento automatizado de sus datos que resulte necesario para el adecuado funcionamiento del REG-AGE se fundamenta en el artículo 6.1 c) y e) del citado Reglamento.

Previo análisis de los riesgos para los derechos y libertades de las personas físicas, se adoptarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales que serán revisadas y actualizadas cuando sea necesario.

Las medidas a implantar como consecuencia del citado análisis de riesgos, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad deberán prevalecer sobre éstas últimas, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos.

La Dirección General de Gobernanza Pública será la responsable del tratamiento, siendo la Secretaría General de Administración Digital la encargada del tratamiento según lo estipulado en el artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos.

**Disposición adicional primera.** *Integración en el REG-AGE.*

Los departamentos ministeriales, organismos públicos y entidades de derecho público vinculados o dependientes se coordinarán con la Secretaría General de Administración Digital para la integración de sus sistemas y plataformas de registro con el REG-AGE.

Las especificaciones técnicas, protocolos y formatos para la integración de sistemas y plataformas en el REG-AGE se publicarán en el Centro de Transferencia Tecnológica (CTT) del Portal de Administración Electrónica.

**Disposición adicional segunda.** *Comunicaciones entre Administraciones Públicas.*

Para los intercambios registrales entre Administraciones Públicas no será de utilización el servicio electrónico de registro accesible desde la sede electrónica del Punto de Acceso General. En su lugar, se podrán utilizar las aplicaciones o sistemas de información para el tratamiento del Registro Electrónico General de cada Administración así como del registro electrónico de cada organismo público o entidad de derecho público vinculado o dependiente, a través del sistema de interconexión de registros (SIR).

El REG-AGE dispondrá de un modelo único de numeración para su empleo en el registro de los asientos por parte de todas las unidades.

**Disposición derogatoria única.** *Derogación normativa.*

Queda derogada la Orden HAP/566/2013, de 8 de abril, por la que se regula el Registro Electrónico Común, y cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta orden.

**Disposición final única.** *Entrada en vigor.*

Esta orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

# § 40

## Orden PCM/1383/2021, de 9 de diciembre, por la que se regula el Registro de Funcionarios Habilitados en el ámbito de la Administración General del Estado, sus Organismos Públicos y Entidades de Derecho Público

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 296, de 11 de diciembre de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-20478

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, consagraba el derecho de la ciudadanía a relacionarse con las Administraciones Públicas por medios electrónicos. Para ello era necesario no solo incorporar las nuevas tecnologías a su funcionamiento interno sino, al mismo tiempo, garantizar a aquellas personas interesadas, que por cualquier motivo no pudiesen acceder electrónicamente a la Administración Pública, disponer de medios adecuados para comunicarse con ella con los mismos derechos y garantías.

El artículo 22 de esa ley preveía que, en aquellos supuestos en los que para la realización de cualquier operación por medios electrónicos se requiriese la identificación o autenticación de la persona interesada mediante algún instrumento de los previstos en el artículo 13, y la persona no dispusiese de ellos, la identificación o autenticación podría ser válidamente realizada por el personal funcionario mediante el uso del sistema de firma electrónica del que estuvieran dotados.

El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, concretaba en su artículo 16 esta habilitación, especificando que para la identificación y autenticación de las personas interesadas por el personal funcionario público, en los servicios y procedimientos en los que resultase necesaria la utilización de sistemas de firma electrónica de los que careciesen, la persona funcionaria habilitada debería disponer de un sistema de firma electrónica admitido por el órgano u organismo público destinatario de la actuación.

La Orden HAP/7/2014, de 8 de enero, del Registro de Funcionarios Habilitados para la identificación y autenticación de ciudadanos, en el ámbito de la Administración General del Estado y sus Organismos públicos vinculados o dependientes, estableció por primera vez la regulación de un registro del personal de funcionario que pudieran asistir a las personas interesadas en la realización de determinados trámites electrónicos de identificación y autenticación en su nombre.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge y amplía esta figura. Así, en línea con la normativa anterior, se establece en su artículo 12 que cuando las personas interesadas, que no estén obligadas a relacionarse electrónicamente con las Administraciones Públicas, no dispongan

de los medios electrónicos necesarios, su identificación o firma electrónica en el procedimiento administrativo podrá ser válidamente realizada por el personal funcionario público mediante el uso del sistema de firma electrónica del que esté dotado para ello.

A estos efectos, se prevé que la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales mantengan actualizado un registro u otro sistema equivalente, donde constará el personal funcionario habilitado para la identificación o firma y en el que se incluirán, al menos, aquellos que presten servicios en las Oficinas de Asistencia en Materia de Registros.

Por otra parte, el artículo 27 de la Ley 39/2015, de 1 de octubre, al regular la validez y eficacia de las copias realizadas por las Administraciones Públicas, prevé que la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales podrán realizar copias auténticas mediante personal funcionario habilitado o mediante actuación administrativa automatizada para lo que deberán mantener actualizado un registro u otro sistema equivalente, donde constará el personal funcionario habilitado para la expedición de copias auténticas. En este artículo también se precisa que en el mismo constará, al menos, el personal funcionario que preste servicios en las Oficinas de Asistencia en Materia de Registros.

La exposición de motivos de la citada ley establece que, si así decide, cada Administración podrá hacer constar en este registro o sistema equivalente conjuntamente el personal funcionario dedicado a asistir a las personas interesadas en el uso de medios electrónicos y el facultado para realizar copias auténticas, no existiendo impedimento a que una misma persona funcionaria tenga reconocida ambas funciones o solo una de ellas.

El Reglamento de actuación y funcionamiento del Sector Publico por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, crea en su artículo 31 el Registro de Funcionarios Habilitados en el ámbito de la Administración General del Estado y sus Organismos públicos y Entidades de derecho público, previendo en su apartado cuarto que la regulación de su funcionamiento se realizará por orden conjunta de las personas titulares del Ministerio de Hacienda y Función Pública y del Ministerio de Asuntos Económicos y Transformación Digital. Además, señala en el segundo apartado que el registro será interoperable con los sistemas equivalentes que ya existan en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.

Conforme a este marco legal y reglamentario, esta orden tiene por objeto regular el funcionamiento del Registro de Funcionarios Habilitados para la expedición de copias auténticas y para la identificación o firma electrónica de las personas interesadas en aquellos procedimientos que se determinen y que estarán disponibles para la ciudadanía en el Punto de Acceso General de la Administración General del Estado.

Esta orden se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. En este sentido, la norma da cumplimiento a los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia. Además, persigue un interés general al pretender incrementar la eficiencia, y la transparencia en el funcionamiento del sector público estatal. No existe ninguna alternativa regulatoria menos restrictiva, resulta coherente con el ordenamiento jurídico y permite una gestión más eficiente de los recursos públicos.

La norma ha sido informada por la Agencia Española de Protección de Datos, en virtud del artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y del artículo 5.3 b) del Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio.

En su virtud, a propuesta conjunta de la Vicepresidenta Primera del Gobierno y Ministra de Asuntos Económicos y Transformación Digital y de la Ministra de Hacienda y Función Pública, dispongo:

**Artículo 1.** *Objeto y ámbito de aplicación.*

De acuerdo con lo previsto en el artículo 31.4 del Reglamento de actuación y funcionamiento del Sector Publico por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, esta orden tiene por objeto la regulación del Registro de

Funcionarios Habilitados, (en adelante, RFH), en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho públicos vinculados o dependientes.

**Artículo 2.** *Órganos competentes.*

1. La Dirección General de Gobernanza Pública del Ministerio de Hacienda y Función Pública asume la gobernanza y gestión del RFH, correspondiendo a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital el diseño, la implantación y la gestión técnica de la plataforma tecnológica que soporte el Registro.

2. La inscripción del personal funcionario que se relaciona en el artículo 3.1 de esta orden corresponde a los titulares de los órganos y unidades donde estos presten servicios.

3. Producida la anotación de la habilitación del personal funcionario, el registro generará una credencial en la que se hará constar su identificación personal y administrativa, los procedimientos y servicios a los que alcanza su habilitación, la fecha de inicio de la misma y, en su caso, su fecha de fin.

**Artículo 3.** *Inscripción en el registro.*

1. En el RFH, regulado por esta orden, deberán inscribirse:

a) El personal funcionario habilitado para realizar la identificación o firma electrónica de las personas interesadas no obligadas a relacionarse electrónicamente con la Administración, conforme a lo previsto en el artículo 12 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en aquellos procedimientos que se determinen por el ministerio, organismo o entidad competente para su tramitación.

b) El personal funcionario habilitado para la expedición de copias auténticas de los documentos públicos administrativos o privados, ya sea en formato papel o electrónico, conforme a lo previsto en el artículo 27 de la Ley 39/2015, de 1 de octubre.

c) El personal funcionario habilitado que presta servicios en las Oficinas de Asistencia en Materia de Registros, que estará habilitado para la identificación o firma electrónica de las personas interesadas en aquéllos procedimientos y servicios que se determinen y para la expedición de copias auténticas electrónicas de cualquier documento en papel que presenten las personas interesadas para que se remitan desde la citada oficina a la unidad competente para su incorporación a un expediente administrativo.

2. Podrán ser habilitados tanto el personal funcionario de carrera como interino, en servicio activo, a que se refiere el artículo 8.2 a) y b) del Texto Refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y presten servicios en la Administración General del Estado o en cualquiera de sus organismos públicos o entidades de derecho público vinculados o dependientes.

**Artículo 4.** *Identificación y firma electrónica.*

1. La persona interesada, previa acreditación de su identidad, deberá dar su consentimiento expreso para su identificación o firma por el personal funcionario habilitado para cada actuación administrativa que la requiera, a través del formulario que se incluye como Anexo I disponible en el Punto de Acceso General electrónico de la Administración General del Estado (https://administracion.gob.es).

2. El personal funcionario habilitado entregará a la persona interesada toda la documentación acreditativa del trámite realizado así como una copia del documento de consentimiento expreso cumplimentado y firmado. A estos efectos, el personal funcionario habilitado utilizará el sistema de firma electrónica del que esté dotado para ello.

**Artículo 5.** *Expedición de copias auténticas.*

1. La habilitación para la expedición de copias auténticas, a la que se refiere el artículo 3.1 b), será conferida por los titulares de los órganos a los que corresponda la emisión de los

documentos originales, su custodia, el archivo de documentos o que en sus normas de competencia así se haya previsto.

2. El personal funcionario que preste servicios en las Oficinas de Asistencia en Materia de Registros está habilitado para la expedición de copias auténticas electrónicas de cualquier documento en papel que presenten las personas interesadas para que se remita desde la citada oficina a la unidad competente para su incorporación a un expediente administrativo.

**Artículo 6.** *Contenido del Registro de Funcionarios Habilitados.*

En el RFH constarán los siguientes datos del personal funcionario habilitado:

a) Documento Nacional de Identidad.
b) Nombre y apellidos.
c) Órgano, organismo o entidad en el que presta servicios, centro directivo y centro de destino identificados mediante su código asignado en el Directorio Común de Unidades Orgánicas y Oficinas, indicándose el código de oficina para el caso de personal funcionario destinado en una Oficina de Asistencia en Materia de Registros.
d) Puesto de trabajo que desempeña.
e) Correo electrónico corporativo
f) Fecha de alta en el RFH.
g) Tipo de habilitaciones: identificación o firma electrónica y/o expedición de copias auténticas.
h) Procedimientos y servicios para los que se tiene autorizada la habilitación, identificados mediante su código asignado en el inventario del Sistema de Información Administrativa.
i) Fecha de baja en el RFH.
j) Causas de las cancelaciones de las habilitaciones.

**Artículo 7.** *Funcionamiento del Registro de Funcionarios Habilitados.*

1. La inscripción como personal funcionario habilitado en el RFH tendrá una duración máxima de cinco años prorrogable de forma expresa por periodos quinquenales sucesivos.

2. La habilitación continuará vigente durante el periodo previsto en el apartado anterior en tanto no se supriman los procedimientos y servicios a los que alcanza su habilitación, o en tanto no se produzca un cambio de puesto de trabajo. Asimismo, la habilitación podrá ser revocada en cualquier momento por el órgano competente para su concesión.

3. Se podrá consultar la base de datos del Registro Central de Personal o sistema equivalente únicamente a efectos de la comprobación de los datos de la situación administrativa y del destino del personal funcionario habilitado.

4. La inscripción de la habilitación continuará vigente hasta que se cancele la misma en el RFH, en los supuestos contemplados en el apartado segundo, o hasta que transcurra el periodo máximo de vigencia sin prórroga expresa.

5. En el Sistema de Información Administrativa deberán constar los procedimientos y servicios para los que pueda conferirse la habilitación incorporada al RFH según determine el órgano responsable de los mismos. La supresión de algún procedimiento o servicio en dicho inventario impedirá su gestión por medio de personal funcionario habilitado y provocará la cancelación de las habilitaciones ligadas al mismo.

6. Se utilizarán los códigos de los procedimientos y servicios administrativos asignados en el inventario del Sistema de Información Administrativa de la Administración General del Estado previsto en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.

**Artículo 8.** *Publicidad de procedimientos.*

En el Punto de Acceso General de la Administración General del Estado se publicará una relación de todos los procedimientos y servicios por medios electrónicos que se determinen expresamente por los departamentos ministeriales, organismos públicos o entidades de derecho público vinculados o dependientes que han sido objeto de habilitación. Respecto a cada uno de los procedimientos y servicios que figuren en dicha relación se hará

constar su descripción, código identificativo y las Oficinas de Asistencia en Materia de Registros u otras dependencias de atención al ciudadano en las que los ciudadanos puedan ejercer el derecho.

**Artículo 9.** *Acceso electrónico al Registro de Funcionarios Habilitados por las Administraciones Públicas.*

1. El RFH será accesible para los órganos de cualquier Administración Pública, sus organismos públicos y entidades de derecho público para obtener información sobre habilitaciones.

2. El registro ofrecerá a los órganos y organismos interesados, como vía de acceso a la información, el acceso en línea mediante servicios web a los efectos de comprobar, automáticamente y en tiempo real desde las aplicaciones, la habilitación de un funcionario para el procedimiento al que den soporte. Las peticiones al registro para los procedimientos y trámites por medios electrónicos, de las que el órgano u organismo administrativo peticionario sea competente, se enviarán por un canal seguro de comunicaciones y deberán firmarse con firma electrónica avanzada cualificada o sello electrónico cualificado del citado órgano o administración de adscripción. La aplicación de soporte al registro mantendrá trazabilidad de todas las peticiones recibidas.

**Artículo 10.** *Protección de Datos de Carácter Personal.*

De conformidad con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, el tratamiento automatizado de sus datos que resulte necesario para el adecuado funcionamiento del RFH se fundamenta en el artículo 6.1 b), c) y d) del citado Reglamento.

Previo análisis de los riesgos para los derechos y libertades de las personas físicas se adoptarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales que serán revisadas y actualizadas cuando sea necesario. Las medidas a implantar como consecuencia del citado análisis de riesgos, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad, deberían prevalecer sobre éstas últimas a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos.

Se adoptarán las medidas que se estimen adecuadas para garantizar que la cancelación de las inscripciones y, en su caso, la rectificación de los datos personales, se realizarán sin dilación teniendo en cuenta que se trata de datos personales correspondientes a funcionarios públicos que se encuentran en poder de la Administración.

**Disposición derogatoria única.** *Derogación normativa.*

Queda derogada la Orden HAP/7/2014, de 8 de enero, por la que se regula el Registro de Funcionarios Habilitados para la identificación y autenticación de ciudadanos en el ámbito de la Administración General del Estado y sus Organismos públicos vinculados o dependientes.

**Disposición final primera.** *Modificación de formularios.*

Corresponde a la persona titular de la Secretaría de Estado de Función Pública la actualización de los formularios previstos en los Anexos I y II de esta orden relativos al consentimiento por parte de la persona interesada para su identificación o firma por la persona funcionaria habilitada, y a la habilitación conferida al personal funcionario, así como la aprobación de otros formularios que, en su caso, resulten precisos para la gestión de dicho Registro.

Estos formularios serán publicados en el Punto de Acceso General de la Administración General del Estado (https://administracion.gob.es).

**Disposición final segunda.** *Entrada en vigor.*

Esta orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

**ANEXO I**

Consentimiento expreso del/la interesado/a para su identificación, y en su caso firma electrónica por /habilitado.

D./D.ª .....

DNI: .....

DECLARA:

QUE NO DISPONE DE LOS MEDIOS ELECTRÓNICOS NECESARIOS PARA SU IDENTIFICACIÓN Y/O FIRMA Y QUE OTORGA SU CONSENTIMIENTO, POR ESTA ÚNICA VEZ, PARA LA IDENTIFICACIÓN O FIRMA POR EL/LA FUNCIONARIO/A HABILITADO/A ABAJO FIRMANTE, PARA LA REALIZACIÓN DEL SIGUIENTE TRÁMITE O ACTUACIÓN ELECTRÓNICA:

- DESCRIPCIÓN DEL TRÁMITE O ACTUACIÓN:
- CÓDIGO SIA[1]:

---

[1] A cumplimentar por la Administración.

EL/LA FUNCIONARIO/A CON IDENTIFICACIÓN:

NOMBRE Y APELLIDOS: …….....

N.º DE CREDENCIAL: ……

En ..... a ..... de ..... de .....

EL/LA INTERESADO/A EL/LA FUNCIONARIO/A HABILITADO/A

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS en cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Responsable del tratamiento: Dirección General de Gobernanza Pública del Ministerio de Hacienda y Función Pública, con domicilio en la calle Manuel Cortina 2, 28010 Madrid.

Encargado del tratamiento: Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

Finalidad: acreditar el consentimiento expreso del ciudadano a la habilitación del funcionario en los términos fijados por el Art. 12 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Legitimación: cumplimiento de una obligación legal (artículo 6.1 e) RGPD.

Destinatarios: Persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO I

Para la cumplimentación y tramitación del consentimiento expreso del/la interesado/a para su identificación y autenticación por personal funcionario público habilitado, se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada actuación electrónica que el/ la interesado/a desee realizar a través del personal funcionario habilitado, consignando, en cada caso, todos los datos que se requieren en el modelo de formulario.

b) En el caso de que se realicen varias acciones sobre un mismo procedimiento, se cumplimentarán tantos ejemplares como acciones se vayan a realizar.

c) Al efectuar la actuación, el personal funcionario habilitado presentará a el/la interesado/a copia impresa de la cumplimentación de datos en el sistema de información que dé soporte al mismo, para que éste dé su conformidad, mediante su firma en el impreso, antes de proceder a completar la actuación.

d) El personal funcionario habilitado entregará al/la interesado/a una copia del documento cumplimentado y firmado por ambas partes.

**ANEXO II**

**Modelo normalizado para la habilitación de los/las funcionarios/as**

D./D.ª .....

DNI .....

TITULAR DE (ÓRGANO COMPETENTE PARA OTORGAR LAS HABILITACIONES)

……

ACREDITO A:

D./D.ª ……

DNI …….....

Correo electrónico corporativo ……..……..

Funcionario/a del Cuerpo ……..……..

Con destino en Ministerio ……..……..

Centro Directivo/Organismo ……..……..

Centro de destino/Oficina ……..……..

Puesto de trabajo ……..……..

☐ Como funcionario/a habilitado/a para la identificación y firma de los/las interesados/as en los procedimientos que se indican a continuación:

Descripción del procedimiento y código SIA

…

☐ Como funcionario/a habilitado/a para la expedición de copias auténticas de los documentos públicos administrativos válidamente emitidos por las Administraciones Públicas:

Descripción del procedimiento y código SIA

…

☐ Como funcionario/a habilitado/a para la expedición de copias electrónicas auténticas de los documentos que presenten los/las interesados/as y se vayan a incorporar a un expediente.

# § 41

## Orden PCM/1384/2021, de 9 de diciembre, por la que se regula el Registro Electrónico de apoderamientos en el ámbito de la Administración General del Estado

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 296, de 11 de diciembre de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-20479

El Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, regula en su artículo 33 el Registro Electrónico de Apoderamientos de la Administración General de Estado y establece en su apartado 4 que mediante orden conjunta de la persona titular del Ministerio de Hacienda y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se regularán los requisitos y condiciones de funcionamiento del mismo.

La creación del Registro Electrónico de Apoderamientos de la Administración General de Estado tiene como finalidad facilitar la acreditación de la representación de las personas interesadas en procedimientos administrativos en los que tengan o puedan tener la condición de persona interesada, previa realización voluntaria de un apoderamiento por comparecencia personal o electrónica apud acta a favor de otra persona para que realice trámites en su nombre, sin coste alguno.

Mediante esta orden se determinan los órganos responsables y el sistema de funcionamiento en el ámbito de la Administración General del Estado, el procedimiento de incorporación de los apoderamientos, así como la revocación, renuncia, vigencia y prórroga de los apoderamientos.

Por otra parte, se aprueban los modelos de poderes inscribibles en el ámbito de la Administración General del Estado y de sus organismos públicos y entidades de derecho público vinculados o dependientes que no cuenten con registro electrónico de apoderamientos propio.

Esta orden se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. En este sentido, la norma da cumplimiento a los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia. La misma persigue un interés general al pretender incrementar la eficiencia, y la transparencia en el funcionamiento del sector público estatal. No existe ninguna alternativa regulatoria menos restrictiva, resulta coherente con el ordenamiento jurídico, y permite una gestión más eficiente de los recursos públicos.

Esta orden ha sido informada por la Agencia Española de Protección de Datos, en virtud del artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y del artículo 5.3.b) del Estatuto de la

Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio.

En su virtud, a propuesta conjunta de la Vicepresidenta Primera del Gobierno y Ministra de Asuntos Económicos y Transformación Digital y de la Ministra de Hacienda y Función Pública, dispongo:

**Artículo 1.** *Objeto y ámbito de aplicación.*

1. Esta orden tiene por objeto regular los requisitos y condiciones de funcionamiento del Registro Electrónico de Apoderamientos de la Administración General del Estado (en adelante, REA-AGE) en el ámbito de la Administración General del Estado y de sus organismos públicos y entidades de derecho público vinculados o dependientes que no cuenten con un registro electrónico de apoderamientos particular.

2. El REA-AGE será accesible desde la sede electrónica del Punto de Acceso General de la Administración General del Estado así como desde las sedes electrónicas asociadas de la Administración General del Estado y las sedes electrónicas o sedes electrónicas asociadas de los organismos públicos o entidades de derecho público vinculados o dependientes.

3. En el REA-AGE se inscribirán los apoderamientos a los que se refiere el artículo 3 otorgados apud acta a favor de la persona representante, presencial o electrónicamente, por quien pueda tener la condición de persona interesada en un procedimiento administrativo.

4. Asimismo esta orden tiene por objeto aprobar los modelos que figuran en los anexos I a V en los que se concretan los actos objeto de inscripción en el REA-AGE que podrán consistir en la inscripción del otorgamiento de poder apud acta; revocación por el poderdante, prórroga de la vigencia del poder, aceptación de la persona apoderada y renuncia del poder por la persona apoderada.

Los modelos se utilizarán para su presentación en papel mediante comparecencia personal en las Oficinas de Asistencia en Materia de Registros de la Administración General del Estado, por personas físicas no obligadas a relacionarse con la Administración por medios electrónicos.

**Artículo 2.** *Órganos competentes.*

1. La Dirección General de Gobernanza Pública del Ministerio de Hacienda y Función Pública asume la gobernanza y gestión funcional del REA-AGE, correspondiendo a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital el diseño, implantación y gestión técnica de la plataforma tecnológica que soporte el registro.

2. En cada ministerio se designará una persona delegada del REA-AGE con rango Subdirector General o asimilado, que desempeñará las funciones previstas en el artículo 6 de esta orden. Se podrá nombrar más de una persona delegada cuando el volumen de actividad o número de Oficinas de Asistencia en Materia de Registros así lo aconseje.

La designación corresponderá a la persona titular de la Subsecretaría o, en su caso, a la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público correspondiente.

**Artículo 3.** *Tipos de apoderamientos y contenido del REA-AGE.*

1. Los poderes que se inscriban en el REA-AGE corresponderán a alguno de los siguientes tipos:

a) Poder general para que la persona apoderada pueda actuar en nombre de la poderdante en cualquier actuación administrativa y ante cualquier Administración Pública, incluidos los organismos públicos o entidades de derecho púbico que cuenten con registro electrónico de apoderamientos particular, conforme a lo previsto en el artículo 6.4.a) de la Ley 39/2015, de 1 de octubre.

b) Poder para que la persona apoderada pueda actuar en nombre de la poderdante en cualquier actuación administrativa ante la Administración General del Estado y/o sus organismos públicos o entidades de derecho público vinculados o dependientes concretos

que no cuenten con registro electrónico de apoderamientos particular, conforme a lo previsto en el artículo 6.4.b) de la Ley 39/2015, de 1 de octubre.

c) Poder, para que la persona apoderada pueda actuar en nombre de la persona poderdante para la realización de determinados trámites especificados en el poder, ante un órgano de la Administración General del Estado o ante un organismo público o entidad de derecho público vinculado o dependiente de la misma que no cuente con registro de apoderamientos particular, conforme a lo previsto en el artículo 6.4.c) de la Ley 39/2015, de 1 de octubre.

2. Cada departamento ministerial u organismo público o entidad de derecho público vinculado o dependiente indicará en el Sistema de Información Administrativa, regulado en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, los trámites que pueden ser objeto de apoderamiento a través del poder previsto en el apartado 1.c).

En la sede electrónica del PAGe (https://sede.administracion.gob.es) figurará una relación pública de dichos trámites.

3. El apoderamiento podrá ser otorgado por varias personas físicas a una persona apoderada que tenga condición de persona física o jurídica.

4. Para inscribir un apoderamiento en el REA-AGE, se hará constar:

a) Nombre y apellidos (para el caso de persona física), denominación o razón social (para el caso de persona jurídica) y Documento Nacional de Identidad, Número de Identificación Fiscal o Número de Identidad de Extranjero de la persona o entidad poderdante.

b) Nombre y apellidos (para el caso de persona física), denominación o razón social (para el caso de persona jurídica) y Documento Nacional de Identidad, Número de Identificación Fiscal o Número de Identidad de Extranjero de la persona apoderada.

c) Tipología del poder.

d) Periodo de vigencia del poder.

e) Fecha de otorgamiento.

f) Número de referencia del alta y fecha de alta en el REA-AGE.

g) Copia del poder otorgado en documento público o privado con firma electrónica o notarialmente legitimada cuando la inscripción se realice a solicitud de la persona apoderada. En este caso constará también su bastanteo, sin perjuicio de la apreciación concreta por los órganos instructores del procedimiento, de su suficiencia en la actuación o procedimiento en que se emplee.

h) Declaración responsable que acredite que se contempla la posibilidad de representar a terceros ante las Administraciones Públicas en los Estatutos de la persona jurídica cuando actúe como persona apoderada.

**Artículo 4.** *Inscripción de los apoderamientos en el REA-AGE.*

1. Cuando la persona poderdante sea persona física no obligada a relacionarse electrónicamente con las Administraciones Públicas, el apoderamiento y su posterior solicitud de inscripción en el REA-AGE podrá realizarlo apud acta mediante su comparecencia personal en una Oficina de Asistencia en Materia de Registros de la Administración General del Estado.

También lo podrá realizar electrónicamente apud acta, en el REA-AGE, mediante el uso de los sistemas de identificación y firma electrónica previstos en los artículos 9 y 10 de la Ley 39/2015 de 1 de octubre.

2. Cuando de acuerdo a lo dispuesto en el artículo 14 de la Ley 39/2015, de 1 de octubre, la persona poderdante se relacione obligatoria o voluntariamente con las Administraciones Públicas por medios electrónicos, la solicitud de inscripción del apoderamiento solo podrá llevarse a cabo electrónicamente, utilizando los medios de identificación y firma electrónica previstos en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre.

En el caso de que la persona poderdante realice la solicitud de inscripción en el REA-AGE en su condición de representante de una persona jurídica, los medios electrónicos

utilizados por aquella permitirán acreditar la representación y capacidad alegadas para realizar las actuaciones ante el mismo.

3. La solicitud de inscripción se presentará en el modelo del anexo I de esta orden en el caso de comparecencia personal, o en el formulario electrónico basado en el anterior cuando se acceda por internet.

La solicitud de inscripción quedará anotada automáticamente en el Registro Electrónico General para constancia de la presentación por la persona interesada.

Si la persona apoderada es persona jurídica se procederá a la inscripción cuando conste la documentación a la que se refiere el artículo 3.4.h).

La inscripción en el REA-AGE solicitada por el poderdante será efectiva en el momento en el que quede inscrita la aceptación por la persona apoderada y haya sido incorporado el bastanteo del poder cuando este sea jurídicamente exigible.

4. La inscripción de apoderamientos en el REA-AGE puede realizarse también a solicitud de la persona apoderada, exigiéndose en este supuesto que aporte una copia o certificación del poder otorgado mediante documento público o privado con firma electrónica o notarialmente legitimada. En el caso de aportar poderes notariales se exigirá un Código Seguro de Verificación (CSV en adelante), para poder acceder al sistema de consulta y conocer el contenido y la situación de vigencia del mismo. Si no se dispone de un CSV, se consignarán los datos identificativos del documento notarial.

Cuando el poder se haya otorgado en documento privado con firma electrónica, la solicitud de inscripción por la persona apoderada solo se podrá presentar por medios electrónicos.

**Artículo 5.** *Aceptación por la persona apoderada.*

1. El poder no surtirá efectos en tanto no se inscriba en el REA-AGE la aceptación de la persona apoderada. Se entenderá la aceptación tácita en el caso de que la solicitud de inscripción la presente la persona apoderada.

2. La aceptación por la persona apoderada se acreditará, surtiendo efectos inmediatos, por cualquiera de los siguientes medios:

a) Por comparecencia personal de la persona física apoderada no obligada a relacionarse con la administración por medios electrónicos. Presentará el modelo del anexo IV en una Oficina de Asistencia en Materia de Registros y el personal funcionario de la oficina entregará un justificante de la presentación a la persona interesada, quedando anotado automáticamente en el Registro Electrónico General.

b) Electrónicamente, mediante el formulario basado en el anexo IV, utilizando los sistemas de identificación y firma electrónica previstos en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, y en el caso de representante de persona jurídica utilizará los medios electrónicos que permitan acreditar la representación y capacidad de actuación necesarios. La aceptación quedará anotada automáticamente en el Registro Electrónico General para constancia de la presentación para la persona interesada.

3. El plazo máximo de aceptación por parte de la persona apoderada no podrá superar los veinte días hábiles desde la fecha de alta de la solicitud de inscripción en el REA-AGE. Transcurrido este periodo, se entenderá que no ha aceptado el apoderamiento.

**Artículo 6.** *Comprobación del contenido del apoderamiento y bastanteo.*

1. Para poder inscribir válidamente un apoderamiento en el REA-AGE la solicitud deberá cumplir todos los requisitos establecidos en el artículo 3.

2. Además, con carácter previo a la inscripción, se realizarán las siguientes comprobaciones:

a) En los apoderamientos cuya inscripción se solicite electrónicamente, la aplicación informática del REA-AGE únicamente permitirá inscribir una solicitud basada en el anexo I que contenga todos los datos requeridos, que vaya acompañada de los documentos que, en su caso, sean preceptivos y se hayan cumplido los requisitos de identificación y firma electrónicas. En aquellos casos en los que se detecten anomalías de tipo técnico, el sistema lo pondrá en conocimiento de la persona interesada a los efectos oportunos.

b) En los apoderamientos otorgados mediante comparecencia personal, el personal funcionario de la Oficina de Asistencia en Materia de Registros de la Administración General del Estado verificará la identidad de la persona compareciente, que el modelo del anexo I está debidamente cumplimentado en todos los apartados aplicables al tipo de apoderamiento de que se trate, así como que se aporta la documentación complementaria que, en su caso, sea necesaria. Se hará constar la identificación de la persona funcionaria ante quien comparece para dar de alta en el REA-AGE los apoderamientos.

3. Cuando la persona apoderada aporte documento público o privado con firma electrónica o notarialmente legitimada, será necesario el bastanteo de los poderes, que se solicitará de la siguiente manera:

a) Cuando se trate de la solicitud de inscripción de un apoderamiento general ante cualquier Administración Pública previsto en el artículo 3.1.a) o de un apoderamiento previsto en el artículo 3.1.b) para actuar ante la Administración General del Estado y todos sus organismos públicos y entidades de derecho público vinculados o dependientes que no cuenten con Registro electrónico de apoderamientos particular la Dirección General de Gobernanza Pública del Ministerio de Hacienda y Función Pública será la responsable de solicitar el bastanteo de los poderes a su servicio jurídico, en los términos que al efecto establezca la Abogacía General del Estado-Dirección del Servicio Jurídico del Estado.

El eventual requerimiento de subsanación de defectos en la representación a la persona interesada, será llevado a cabo por la Dirección General de Gobernanza Pública, concediendo un plazo de diez días hábiles para que se subsane la falta o acompañe los documentos preceptivos con indicación de que, si así no lo hiciera, se le tendrá por desistido de su solicitud de inscripción, previa resolución que deberá ser dictada en los términos previstos en los artículos 21 y 68 de la Ley 39/2015, de 1 de octubre.

b) Cuando se trate de la solicitud de inscripción de un apoderamiento previsto en el artículo 3.1.b) o en el artículo 3.1.c), para actuar ante un organismo público o entidad de derecho público concreto vinculado o dependiente de la Administración General del Estado que no cuente con registro electrónico de apoderamientos propio, o de la inscripción de un apoderamiento previsto en el párrafo c) del artículo 3.1 para actuar ante un ministerio, organismo o entidad concreto que no cuente con registro electrónico de apoderamientos propio, se procederá en la forma señalada en el apartado anterior, siendo la persona delegada del REA-AGE del ministerio, organismo o entidad al que esté adscrito el órgano competente de los trámites objeto del apoderamiento, el responsable de solicitar el bastanteo de los poderes al servicio jurídico correspondiente, en los términos que al efecto establezca la Abogacía General del Estado-Dirección del Servicio Jurídico del Estado y, en su caso, requerir la subsanación de defectos.

**Artículo 7.** *Revocación y renuncia del apoderamiento.*

1. La inscripción de la revocación por la persona poderdante o de la renuncia por la persona apoderada de un apoderamiento inscrito en el REA-AGE se acreditará aportando los modelos previstos en los anexos II y III, respectivamente, o sus equivalentes electrónicos, surtiendo efecto en ambos casos desde la fecha de su inscripción.

2. La solicitud de inscripción en el REA-AGE se llevará a cabo en la misma forma prevista en el artículo 5.2 para la aceptación de un poder.

**Artículo 8.** *Vigencia y prórroga del apoderamiento.*

1. El apoderamiento tendrá una vigencia máxima de cinco años a contar desde la fecha de su inscripción en el REA-AGE.

2. En cualquier momento antes de la finalización del plazo de vigencia la persona poderdante podrá prorrogarlo y solicitar la inscripción de dicha prórroga, utilizando para ello el modelo previsto en el anexo V o su equivalente electrónico, según corresponda, y por los mismos medios previstos en el artículo 5.2.

3. Las prórrogas tendrán una vigencia máxima de cinco años a contar desde la fecha su inscripción en el REA-AGE.

**Artículo 9.** *Consultas por la persona interesada.*

El REA-AGE no tiene carácter público por lo que solo la persona interesada, una vez identificada, podrá consultar el REA-AGE electrónica o presencialmente, según corresponda, y acceder a la información de los apoderamientos de los que sea poderdante o apoderada.

**Artículo 10.** *Consultas por los órganos de la Administración General del Estado, organismos públicos o entidades de derecho público vinculados o dependientes.*

1. El REA-AGE permitirá la consulta de los órganos, organismos públicos y entidades de derecho público interesados a los efectos de comprobar que un apoderamiento está vigente.

2. Las peticiones de consulta al REA-AGE, relativas a los apoderamientos vigentes y válidos para los procedimientos por medios electrónicos de las que el órgano administrativo peticionario sea competente, se enviarán por un canal seguro de comunicaciones y deberán firmarse con firma electrónica avanzada cualificada o sello electrónico cualificado del citado órgano o administración de adscripción. La aplicación de soporte mantendrá trazabilidad de todas las peticiones recibidas.

3. Las consultas se limitarán a los datos estrictamente necesarios para verificar la existencia, vigencia y alcance de los poderes en relación con las concretas actuaciones administrativas que se pretenden realizar y para poder comunicarse con la persona representante.

**Artículo 11.** *Protección de Datos de Carácter Personal.*

1. De conformidad con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando la persona poderdante o la apoderada tuvieran condición de personas físicas, el tratamiento automatizado de sus datos que resulte necesario para el adecuado funcionamiento del REA-AGE se fundamenta en el artículo 6.1.e) del reglamento.

2. Previo análisis de los riesgos para los derechos y libertades de las personas físicas, se adoptarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales que serán revisadas y actualizadas cuando sea necesario.

Las medidas a implantar como consecuencia del análisis de riesgos, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad deberán prevalecer sobre estas últimas, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de protección de datos.

3. La Dirección General de Gobernanza Pública será la responsable del tratamiento, siendo la Secretaría General de Administración Digital la encargada del tratamiento según lo estipulado en el artículo 28 del Reglamento general de protección de datos.

**Artículo 12.** *Interoperabilidad del Registro.*

El REA-AGE deberá ser plenamente interoperable con los registros electrónicos de apoderamientos generales y particulares pertenecientes a todas y cada una de las administraciones garantizando su interconexión, compatibilidad informática, así como la transmisión electrónica de las solicitudes, escritos y comunicaciones que se incorporen al mismo, de acuerdo con lo previsto en el artículo 6.2 de la Ley 39/2015, de 1 de octubre.

**Disposición adicional primera.** *Entidades sin personalidad jurídica.*

Las previsiones que se contienen en esta orden sobre las personas jurídicas serán aplicables, a las entidades sin personalidad jurídica, que solo podrán actuar como poderdantes.

**Disposición adicional segunda.** *Actualización de modelos normalizados.*

Corresponde a la persona titular de la Secretaría de Estado de Función Pública, la actualización de los formularios previstos en los anexos I, II, III, IV y V de esta orden para su

presentación en papel y de sus equivalentes en formato electrónico, así como la aprobación de otros formularios que, en su caso, resulten precisos para la gestión de dicho registro.

Estos formularios serán publicados en el Punto de Acceso General de la Administración General del Estado (https://administracion.gob.es).

**Disposición adicional tercera.** *Comunicación previa de creación de un Registro Electrónico de Apoderamientos particular.*

Los organismos públicos y entidades de derecho público estatales que a la entrada en vigor de esta orden no cuenten con un Registro Electrónico de Apoderamientos particular y decidan crearlo con posterioridad, deberán comunicarlo a la Dirección General de Gobernanza Pública y a la Secretaría General de Administración Digital con una antelación mínima de un mes a la fecha prevista de entrada en funcionamiento para garantizar su interoperabilidad técnica y que se puedan realizar los ajustes necesarios sin merma del servicio.

**Disposición derogatoria única.** *Derogación normativa.*

Quedan derogadas todas las normas de igual o inferior rango en lo que contradigan o se opongan a lo dispuesto en esta orden. En particular, quedan derogadas la Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos y la Orden HFP/633/2017, de 28 de junio, por la que se aprueban los modelos de poderes inscribibles en el Registro Electrónico de Apoderamientos de la Administración General del Estado y en el Registro Electrónico de Apoderamientos de las Entidades Locales y se establecen los sistemas de firma válidos para realizar los apoderamientos apud acta a través de medios electrónicos.

**Disposición final única.** *Entrada en vigor.*

Esta orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

**ANEXO I**

## Inscripción del Poder[1]

Presentado en la Oficina de Asistencia en Materia de Registros n.º[2] _____; ante funcionario/a con N.R.P[2]:_____

Comparece/n: ☐ Poderdante/s ☐ Apoderado/a

1) Identificación de las personas poderdantes

Persona física mayor de edad:

| | | |
|---|---|---|
| DNI/NIE: | | |
| Nombre: | 1.º apellido: | 2.º apellido: |
| Teléfono: | Correo electrónico: | |
| Domicilio: | | |

*Nota: En el caso de apoderamientos de varias personas físicas (poderdantes) a una persona física o jurídica, incluir los datos identificativos anteriores de cada uno de ellos.*

2) La/las persona/s poderdante/s otorga/n poder a favor de la persona apoderada (elija una de las dos opciones)

☐ Persona física mayor de edad:

| | | |
|---|---|---|
| DNI/NIE: | | |
| Nombre: | 1.º apellido: | 2.º apellido: |
| Teléfono: | Correo electrónico: | |
| Domicilio: | | |

[1] La presentación de este modelo en papel en una Oficina de Asistencia en Materia de Registros sólo será posible en el caso de comparecencia de poderdante o apoderado/a persona física.
[2] A cumplimentar por la Administración.

☐ Persona jurídica:

| Identificación de la persona jurídica | |
|---|---|
| NIF: | |
| Denominación social: | |
| Teléfono: | Correo electrónico: |

3) Poder

Tan amplio y bastante como en Derecho sea necesario para actuar en nombre de la persona poderdante para la realización de las siguientes actuaciones (señale uno de los tres tipos de poderes):

☐ A) Poder general para que la persona apoderada pueda actuar en nombre del poderdante en cualquier actuación administrativa y ante cualquier Administración Pública.

☐ B) Poder para que la persona apoderada pueda actuar en nombre de la persona poderdante en cualquier actuación administrativa (elija una opción y complete los datos):

☐ Opción 1: Ante la Administración General del Estado y todos los organismos públicos o entidades de derecho público vinculados o dependientes[3].

☐ Opción 2: Ante un Organismo público o Entidad de derecho público vinculado o dependiente concreto[3].

| *(Denominación del organismo o entidad)* | Código DIR3[4]: |
|---|---|
| | |

[3] Organismos públicos y entidades de derecho público vinculados o dependientes que no cuenten con un Registro Electrónico de Apoderamientos particular. Puede consultar estos organismos a través del Punto de Acceso General de la Administración General del Estado (http://administracion.gob.es) o en el 060.

[4] Los códigos DIR3 serán cumplimentados por la Administración.

☐ C) Poder para que la persona apoderada pueda actuar en nombre de la persona poderdante únicamente para la realización de los siguientes trámites ante un órgano, Organismo público o Entidad de derecho público vinculado o dependiente.

| *(Denominación del órgano, organismo o entidad)* | Código DIR3: |
|---|---|
| Trámites[5] del órgano, organismo o entidad:<br>(para seleccionar todos los trámites escriba la palabra TODOS[6] )<br>…… | Códigos SIA:<br>…… |

4) Vigencia del poder

La vigencia máxima no podrá superar los cinco años a contar desde la fecha de inscripción. La fecha de inicio consignada tendrá valor siempre que sea posterior a la fecha de inscripción.

| Fecha de inicio: / / | Fecha fin: / / |
|---|---|

5) En caso de aportarse documento público o privado con firma legitimada notarial[7]

Debe hacerse constar los siguientes datos:

| Código Seguro de Validación (CSV): |
|---|

[5] Puede consultar el listado de trámites objeto de apoderamiento a través del Punto de Acceso General de la Administración General del Estado (http://administracion.gob.es) o en el 060.
[6] Se refiere a todos los trámites que pueden ser objeto de apoderamiento.
[7] Sólo se aportarán estos datos en el caso de solicitud presentada por persona apoderada.

En caso de no aportar un CSV, datos del poder notarial:

| | | |
|---|---|---|
| Nombre: | 1.º apellido: | 2.º apellido: |
| Colegio: | | |
| N.º Protocolo: | Fecha de otorgamiento: / / | |
| Teléfono: | Correo electrónico: | |
| Dirección: | | |

☐ Poder notarial: Se adjunta documento notarial debidamente firmado.

6) Firma dela persona apoderada[8]

Con la firma del presente escrito acepta la representación conferida.

En _____, __/_____/_____

7) Firma de la/las persona/s poderdante/s[9]

En _____, __/_____/_____

[8] Cuando la solicitud sea presentada por el/la poderdante, la persona apoderada podrá realizar la aceptación en el mismo momento de presentación o, en otro momento, aportando el modelo del Anexo IV en papel debidamente cumplimentado y firmado; o a través de internet.
[9] En el caso de apoderamientos otorgados mediante documento público o privado con firma legitimada notarial no será necesaria la firma de poderdante o poderdantes.

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES

En cumplimiento del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Finalidad: gestión de solicitudes de inscripción de poderes y la acreditación de la representación en los términos de los artículos 11 y 12 de la orden.

Legitimación: cumplimiento de una obligación legal [art. 6.1.e)] RGPD.

Destinatarios: persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

Más información sobre protección de datos en el Punto de Acceso General.

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO I

Para la cumplimentación y tramitación de la inscripción, se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada apoderamiento que el/la ciudadano/a (persona física) desee realizar ante el/la funcionario/a de la Oficina de Asistencia en Materia de Registros, consignando, en cada caso, todos los datos que se requieren en el presente modelo de formulario.

b) El/la funcionario/a de la oficina entregará al/la ciudadano/a un justificante registrado y sellado con la fecha y el número del registro de entrada correspondiente.

c) Los datos de teléfono y correo electrónico se utilizarán para contactar con el/la interesado/a. En el caso de personas físicas, estos datos son opcionales.

**ANEXO II**

## Revocación de poder[10]

Presentado en la Oficina de Asistencia en Materia de Registros n.º[11] _____; ante funcionario/a con NRP[11]:_____

1) Comparece la persona poderdante

Persona física mayor de edad:

| DNI/NIE: | | |
|---|---|---|
| Nombre: | 1.º apellido: | 2.º apellido: |

La persona poderdante REVOCA el poder otorgado en fecha __/__/____, con número: _____, otorgado en favor de la persona apoderada (elija una de las opciones):

☐ Persona física mayor de edad:

| DNI/NIE: | | |
|---|---|---|
| Nombre: | 1.º apellido: | 2.º apellido: |

☐ Persona jurídica:

| Identificación de la persona jurídica |
|---|
| NIF: |
| Denominación social: |

2) Firma de la persona poderdante

En _____, __/_____/_____

[10] La presentación de este modelo en papel ante una Oficina de Asistencia en Materia de Registros sólo será posible en el caso de poderdante persona física.

[11] A cumplimentar por la Administración.

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES en cumplimiento del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Finalidad: gestión de solicitudes de inscripción de poderes y la acreditación de la representación en los términos de los artículos 11 y 12 de la orden.

Legitimación: cumplimiento de una obligación legal [art. 6.1.e)] RGPD.

Destinatarios: persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

Más información sobre protección de datos en el Punto de Acceso General de la Administración General del Estado.

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO II

Se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada revocación que el/la ciudadano/a desee realizar ante el/la funcionario/a de la Oficina de Asistencia en Materia de Registros, consignando, en cada caso, todos los datos que se requieren en el presente modelo de formulario.

b) El/la funcionario/a de la oficina entregará al/la ciudadano/a un justificante registrado y sellado con la fecha y el número del registro de entrada correspondiente.

**ANEXO III**

## Renuncia del poder[12]

Presentado en la Oficina de Asistencia en Materia de Registros n.º[13] _____; ante funcionario/a con NRP[13]:_____.

1) Comparece la persona apoderada

Persona física mayor de edad:

| DNI/NIE: | | |
|---|---|---|
| Nombre: | 1.º apellido: | 2.º apellido: |

El/la apoderado/a RENUNCIA al poder otorgado en fecha: __/__/____, con número: _____, otorgado a su favor, por la persona poderdante:

☐ Persona física mayor de edad:

| DNI/NIE: | | |
|---|---|---|
| Nombre: | 1.º apellido: | 2.º apellido: |

2) Firma de la persona apoderada

En _____, __/_____/_____

[12] La presentación de este modelo en papel ante una Oficina de Asistencia en Materia de Registros solo será posible en el caso de apoderado/a persona física que actúe en nombre de otra persona física no obligada a relacionarse electrónicamente.

[13] A cumplimentar por la Administración.

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES en cumplimiento del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Finalidad: gestión de solicitudes de inscripción de poderes y la acreditación de la representación en los términos de los artículos 11 y 12 de la orden.

Legitimación: cumplimiento de una obligación legal [art. 6.1.e)] RGPD.

Destinatarios: persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

Más información sobre el Registro Electrónico de Apoderamientos y protección de datos en la sede del Punto de Acceso General de la Administración General del Estado.

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO III

Se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada renuncia que el/la ciudadano/a desee realizar ante el/la funcionario/a de la Oficina de Asistencia en Materia de Registros, consignando, en cada caso, todos los datos que se requieren en el presente modelo de formulario.

b) El/la funcionario/a de la oficina entregará al/la ciudadano/a un justificante registrado y sellado con la fecha y el número del registro de entrada correspondiente.

**ANEXO IV**

## Aceptación por la persona apoderada[14]

Presentado en la Oficina de Asistencia en Materia de Registros n.º[15] _____; ante funcionario/a con NRP[15]:_____.

1) Comparece la persona apoderada.

Persona física mayor de edad:

| DNI/NIE: | | |
|---|---|---|
| Nombre: | 1.º apellido: | 2.º apellido: |

El/la apoderado/a ACEPTA el poder otorgado en fecha: __/__/____, con número: _____, a su favor, por la persona poderdante:

☐ Persona física mayor de edad:

| DNI/NIE: | | |
|---|---|---|
| Nombre: | 1.º apellido: | 2.º apellido: |

2) Firma de la persona apoderada

Con la firma del presente escrito acepta la representación conferida.

En _____, __/_____/_____

[14] La presentación de este modelo en papel, ante una Oficina de Asistencia en Materia de Registros, sólo será posible en el caso de apoderado/a persona física.
[15] A cumplimentar por la Administración.

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES en cumplimiento del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Finalidad: gestión de solicitudes de inscripción de poderes y la acreditación de la representación en los términos de los artículos 11 y 12 de la orden.

Legitimación: cumplimiento de una obligación legal [art. 6.1 e)] RGPD.

Destinatarios: persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

Más información sobre protección de datos en el Punto de Acceso General de la Administración General del Estado.

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO IV

Se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada aceptación que el/la ciudadano/a desee realizar ante el/la funcionario/a de la Oficina de Asistencia en Materia de Registros, consignando, en cada caso, todos los datos que se requieren en el presente modelo de formulario.

b) El/la funcionario/a de la oficina entregará al/la ciudadano/a un justificante registrado y sellado con la fecha y el número del registro de entrada correspondiente.

**ANEXO V**

## Prórroga de un Poder[16]

Presentado en la Oficina de Asistencia en Materia de Registros nº[17] _____; ante funcionario/a con N.R.P[17]:_____.

1) Comparece la persona poderdante. Persona física mayor de edad:

| | | |
|---|---|---|
| DNI/NIE: | | |
| Nombre: | 1.º apellido: | 2.º apellido: |

El poderdante PRORROGA el poder otorgado en fecha __/__/____, con número: _____, en favor de la persona apoderada (elija una de las opciones):

☐ Persona física mayor de edad:

| | | |
|---|---|---|
| DNI/NIE: | | |
| Nombre: | 1.º apellido: | 2.º apellido: |

☐ Persona jurídica:

| |
|---|
| Identificación persona jurídica |
| NIF: |
| Denominación social: |

La vigencia máxima no podrá superar los cinco años a contar desde la fecha de inscripción.

2) Prórroga del poder hasta[18]: / /

[16] La presentación de este modelo en papel ante una Oficina de Asistencia en Materia de Registros sólo será posible en el caso de poderdante persona física.

[17] A cumplimentar por la Administración.

[18] La vigencia del poder, incluidas las prórrogas, no podrá exceder de 5 años desde la fecha de inscripción.

3) Firma de la persona poderdante

En _____, __/_____/_____

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES en cumplimiento del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Finalidad: gestión de solicitudes de inscripción de poderes y la acreditación de la representación en los términos de los artículos 11 y 12 de la orden.

Legitimación: cumplimiento de una obligación legal [art. 6.1.e)] RGPD.

Destinatarios: persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

Más información sobre protección de datos en el Punto de Acceso General de la Administración General del Estado.

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO V

Se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada prórroga que el/la ciudadano/a desee realizar a ante el/la funcionario/a de la Oficina de Asistencia en Materia de Registros, consignando, en cada caso, todos los datos que se requieren en el presente modelo de formulario.

b) El/la funcionario/a de la oficina entregará al/la ciudadano/a un justificante registrado y sellado con la fecha y el número del registro de entrada correspondiente.

# § 42

## Orden PRE/3949/2006, de 26 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Identidad

Ministerio de la Presidencia
«BOE» núm. 310, de 28 de diciembre de 2006
Última modificación: sin modificaciones
Referencia: BOE-A-2006-22786

Actualmente, en la mayoría de las relaciones de los ciudadanos con la Administración éstos deben presentar una fotocopia de su documento de identidad, ya sea su DNI, si se trata de un ciudadano español o su tarjeta equivalente para el caso de extranjeros residentes en territorio español.

Se estima que el número de fotocopias de documentos acreditativos de la identidad de un ciudadano presentadas anualmente en los trámites administrativos asciende a más de cuatro millones.

El 28 de abril de 2006, el Consejo de Ministros aprobó el Real Decreto 522/2006, de 28 de abril, por el que se suprime la aportación de fotocopias de documentos de identidad en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes.

Los objetivos de dicha norma son, por un lado, suprimir la obligación de presentar fotocopias de los documentos acreditativos de identidad en todos los trámites administrativos, pudiendo sustituirse dicha fotocopia, en aquellos supuestos donde la constancia de los datos fuese imprescindible, por una consulta telemática a la Dirección General de la Policía y de la Guardia Civil de forma directa o diferida; y por otro dotar de mayor seguridad al método actual de verificación de la identidad de un ciudadano, ya que es más fácil manipular una fotocopia que suplantar la identidad del sistema de verificación de datos de identidad basado en la información preservada por la Dirección General de la Policía y de la Guardia Civil.

A partir de la puesta en funcionamiento de este sistema es el propio Departamento ante el que se solicita el trámite el encargado de comprobar, de oficio, la identidad del interesado. Esta consulta se realizará, en los casos en los que sea estrictamente necesario y tras obtener la autorización del interesado. La consulta se realizará con máximas garantías de seguridad y preservando la privacidad de los datos. En caso de que el interesado no dé su consentimiento a realizar esa consulta, deberá aportar su correspondiente fotocopia del Documento Nacional de Identidad.

El objeto de la presente Orden Ministerial es dar cumplimiento al mandato contenido en la disposición final primera del citado Real Decreto 522/2006, de 28 de abril, en virtud del cual el establecimiento de la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Identidad, así como la fecha en que dicho

sistema estará plenamente operativo, se llevará a cabo mediante orden, a propuesta conjunta de los Ministros del Interior y de Administraciones Públicas.

A tal fin, se han tenido en consideración las experiencias previas, las implicaciones técnicas, la búsqueda de racionalidad y sencillez de uso y el aprovechamiento de las ventajas de las economías de escala.

En su virtud, previo respectivos informes favorables del Consejo Superior de Administración Electrónica y de la Agencia de Protección de Datos, a propuesta de los Ministros del Interior y de Administraciones Públicas, dispongo:

**Primero.**

Se aprueba el Reglamento Técnico del Sistema de Verificación de Datos de Identidad, que figura como anexo a la presente Orden Ministerial, como instrumento que establece la configuración, características, requisitos y procedimientos de acceso al citado Sistema.

**Segundo.**

Se fija como fecha de operatividad del Sistema de Verificación de Datos de Identidad el uno de enero de 2007, a partir de la cual no podrá exigirse por la Administración General del Estado o por los Organismos vinculados o dependientes de aquella la aportación de fotocopias del Documento Nacional de Identidad o de los documentos acreditativos de la identidad de extranjeros residentes en España o tarjeta equivalente, salvo en los supuestos previstos en el Real Decreto 522/2006, de 28 de abril.

**Tercero.**

La presente Orden Ministerial se aprueba en aplicación de lo dispuesto en la disposición final primera del Real Decreto 522/2006, de 28 de abril, por el que se suprime la aportación de fotocopias de documentos de identidad en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes. Lo dispuesto en esta Orden Ministerial se aplicará en todo caso de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa aplicable en esta materia.

**Disposición final primera.** *Aplicación y desarrollo.*

1. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio del Interior y previo informe del Consejo Superior de Administración Electrónica, se establecerán los parámetros de calidad de la prestación del servicio del Sistema de Verificación de Datos de Identidad y de cumplimiento de los requisitos y condiciones establecidas en la presente Orden Ministerial. A estos efectos, el Ministerio de Administraciones Públicas establecerá instrumentos de validación y vigilancia del cumplimiento de lo establecido en el párrafo anterior, sin perjuicio de las competencias de los Órganos de Control Interno.

2. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio del Interior y previo informe del Consejo Superior de Administración Electrónica, se podrá proceder a la actualización o modificación del Reglamento Técnico que se aprueba por la presente Orden Ministerial.

3. Se faculta a los Subsecretarios de los departamentos Ministeriales, a los Presidentes de los Organismos Públicos o a los responsables ministeriales correspondientes, para la adopción de las instrucciones o medidas que resulten adecuadas para garantizar el acceso y la utilización del Sistema de Verificación de Datos de Identidad por los órganos y unidades correspondientes a su ámbito.

**Disposición final segunda.** *Entrada en vigor.*

La presente Orden Ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

**ANEXO**

**Reglamento Técnico del Sistema de Verificación de Datos de Identidad**

**Primero.** *Descripción del Sistema de Verificación de Datos de Identidad.*

El Sistema de Verificación de Datos de Identidad puesto a disposición de los Departamentos y Organismos de la Administración General del Estado por parte del Ministerio de Administraciones Públicas se establece como servicio horizontal para la consulta y comprobación de los datos del Documento de Identificación del Ciudadano custodiados por la Dirección General de la Policía y de la Guardia Civil en base a lo dispuesto en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, que atribuye al Cuerpo Nacional de Policía, la función de expedición del Documento Nacional de Identidad y el control de entrada y salida del territorio nacional de españoles y extranjeros. Información que se encuentra registrada y custodiada en los ficheros de la Dirección General de la Policía y de la Guardia Civil, que soportan la gestión del documento nacional de identidad y la Tarjeta de Identificación de Extranjeros (Sus denominaciones, conforme a las Órdenes INT/1751/2002, de 20 de junio e INT/2190/2006, de 19 de junio, son ADDNIFIL y ADEXTTRA, respectivamente).

**Segundo.** *Adopción de medidas de seguridad, organizativas o técnicas de los organismos y aplicaciones que accedan al Sistema de Verificación de Datos de Identidad.*

1. Con carácter general los organismos que accedan al Sistema de Verificación de Datos de Identidad cumplirán con las medidas de seguridad, conservación y normalización que se detallan en los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades aprobados por el Consejo Superior de Administración Electrónica mediante Resolución de 26 de mayo de 2003 y revisiones posteriores.
2. El alcance e intensidad de aplicación de las medidas de seguridad, conservación y normalización vendrán determinadas por el resultado del análisis y gestión de riesgos que se realice, recomendándose a estos efectos la utilización de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) del Consejo Superior de Administración Electrónica.
3. Lo dispuesto en esta Orden Ministerial se aplicará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en el Reglamento de Medidas de Seguridad de los ficheros automatizados de datos de carácter personal aprobado por Real Decreto 994/1999, de 11 de junio.

**Tercero.** *Acceso al Sistema de Verificación de Datos de Identidad.*

1. El acceso al Sistema de Verificación de Datos de Identidad se realizará a través del Sistema de Aplicaciones y Redes para las Administraciones Públicas, siguiendo el esquema de conexión que ésta tiene establecido para cualquier organismo público. Sólo en casos debidamente justificados y previa aprobación, por parte de la Secretaría del Consejo Superior de Administración Electrónica, de un plan para la ordenación de las comunicaciones se habilitarán temporalmente mecanismos de conexión alternativos.
2. El Sistema de Verificación de Datos de Identidad presentará dos formas alternativas de acceso para realizar las correspondientes consultas sobre la veracidad de ciertos datos de identidad:

Un interfaz accesible a través de un navegador de Internet, conforme al RFC 2616: Protocolo de Transferencia de Hipertexto - HTTP/1.1 del IETF, donde un empleado público, debidamente acreditado e identificado, podrá realizar consultas con sólo disponer de un navegador con acceso al Sistema de Aplicaciones y Redes para las Administraciones Públicas y firma electrónica.

Un interfaz automatizado de servicio web, conforme al estándar WSDL 1.1 o superior del W3C cuya definición inicial, y sucesivas actualizaciones, serán puestas a disposición de los Organismos a través del Consejo Superior de Administración Electrónica y su Comisión Permanente.

**Cuarto.** *Requisitos de autenticidad para el acceso al Sistema de Verificación de Datos de Identidad.*

1. Los accesos al Sistema de Verificación de Datos de Identidad se efectuarán utilizando certificados electrónicos reconocidos.
2. Los certificados electrónicos que se utilicen para identificarse ante el Sistema de Verificación de Datos de Identidad deberán ser certificados reconocidos que cumpla la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 9594-8 de 1997).
3. No podrán utilizarse certificados electrónicos caducados o revocados para acceder al Sistema de Verificación de Datos de Identidad.

**Quinto.** *Requisitos de confidencialidad del Sistema de Verificación de Datos de Identidad.*

1. El Sistema de Verificación de Datos de Identidad ofrecerá consultas en las que, a partir del Número del Documento de Identificación del Ciudadano o Extranjero, se devolverá el total, o un subconjunto, de los datos incorporados en dicho documento:

Nombre y apellidos del titular del documento.
Lugar y fecha de nacimiento.
Nombre de los padres.
Sexo.
Estado de vigencia del Documento.

El conjunto de datos a los que tenga acceso cada usuario del sistema será establecido, previa autorización y justificación, por parte del responsable en la Organización Administrativa.
2. Sólo organismos públicos debidamente autorizados tendrán acceso al Sistema de Verificación de Datos de Identidad. En todo organismo público existirá un responsable o administrador delegado del sistema que autorizará los accesos al Sistema de Verificación de Datos de Identidad.
3. Para realizar la consulta al Sistema de Verificación de Datos de Identidad, será preciso el consentimiento del interesado cuyos datos se vayan a verificar, salvo que una norma con rango de ley autorice dicha consulta. Dicho consentimiento deberá constar en la solicitud de iniciación del procedimiento, o en cualquier otra comunicación posterior, siempre y cuando dicha comunicación sea previa a la consulta en el sistema, no pudiendo realizarse consulta alguna en caso de no contar con el consentimiento de forma fehaciente. Los impresos o formularios electrónicos de solicitudes de iniciación de procedimientos administrativos deberán adecuarse para recoger dicho consentimiento.
4. La consulta y el acceso a la información proporcionada por el Sistema de Verificación de Datos de Identidad deberá realizarse con una finalidad concreta, que quedará recogida en el momento de la consulta.

**Sexto.** *Requisitos de integridad de la información proporcionada por el Sistema de Verificación de Datos de Identidad.*

Todas las consultas que se realicen al Sistema de Verificación de Datos de Identidad, así como las respuestas que devuelva el propio sistema, deberán haber sido firmadas electrónicamente. Esta firma electrónica tiene por objeto garantizar la integridad de los datos intercambiados como la identidad de las partes que intervienen y el no repudio de la consulta.

De la misma forma, todas las consultas que el Sistema de Verificación de Datos de Identidad deba realizar a la Dirección General de la Policía y de la Guardia Civil, así cómo las correspondientes respuestas obtenidas resultado de las mismas, habrán de ser debidamente firmadas electrónicamente para garantizar tanto la integridad de la información como la identidad de ambos organismos.

**Séptimo.** *Requisitos de disponibilidad de la información proporcionada por el Sistema de Verificación de Datos de Identidad.*

El Sistema de Verificación de Datos de Identidad estará disponible los 7 días de la semana las 24 horas del día.

**Octavo.** *Garantías jurídicas del Sistema de Verificación de Datos de Identidad ante posibles recursos.*

1. El servicio web proporcionado por este sistema sigue el estándar de intercambio de datos definido por «Sustitución de Certificados en Soporte Papel» del Consejo Superior de Administración Electrónica, que reúne, en base a la normativa vigente, las garantías jurídicas aplicables al intercambio de datos entre Administraciones Públicas.

2. El Sistema de Verificación de Datos de Identidad dispondrá de un módulo de auditoría, en el que quedarán registradas todas las consultas de datos de identidad realizadas, información de contexto asociada, como la identidad del solicitante, la fecha y la finalidad de la consulta, y aquellos eventos relevantes desencadenados a partir de la propia consulta. Se garantizará la integridad y no repudio de la información registrada mediante técnicas de firma electrónica y sellado de tiempo, estableciéndose, asimismo, medidas técnicas para garantizar la disponibilidad y recuperación de aquella información que no se mantenga on-line por motivos de eficiencia técnica o seguridad.

3. Para certificar la fecha y tiempo de las actividades y sucesos registrados en el Sistema de Verificación de Datos de Identidad se hará uso del Servicio de Sellado de Tiempo de la Plataforma de Firma Electrónica del Ministerio de Administraciones Públicas, sincronizada con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara el Laboratorio de la Armada como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

4. Sólo personal de la Administración Pública debidamente autorizado y acreditado podrá acceder a las funcionalidades de auditoría del Sistema de Verificación de Datos de Identidad.

**Noveno.** *Condiciones de la prestación del servicio.*

1. La gestión del Sistema de Verificación de Datos de Identidad corresponde al Ministerio de Administraciones Públicas.

2. Los organismos públicos que hagan uso de este servicio estarán sujetos a las medidas de seguridad, los requisitos de autenticidad, integridad, confidencialidad, disponibilidad y criterios técnicos establecidos en esta Orden Ministerial.

3. Para poder acceder al Sistema de Verificación de Datos de Identidad, los Organismos Administrativos deberán designar a un responsable, tal y como se indica en el apartado segundo del punto quinto del presente anexo técnico, que será el encargado de autorizar a los accesos en su organismo. El nombramiento y cese de este responsable deberá ser comunicado al Ministerio de Administraciones Públicas, para la asignación de los permisos adecuados de acceso al sistema o la cancelación de los mismos.

# § 43

## Orden PRE/4008/2006, de 27 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Residencia

Ministerio de la Presidencia
«BOE» núm. 1, de 1 de enero de 2007
Última modificación: sin modificaciones
Referencia: BOE-A-2007-1

Actualmente, en la mayoría de las relaciones de los ciudadanos con la Administración, éstos deben indicar su lugar de residencia con un nivel de rigurosidad que varía desde la declaración expresa hasta la presentación de un certificado de empadronamiento expedido por el municipio en el cual están registrados sus datos de empadronamiento.

Se estima que el número de documentos acreditativos de la residencia expedidos anualmente asciende a más de diez millones de los cuales más de tres millones han sido solicitados, a su vez, por la Administración.

El 28 de abril de 2006, el Consejo de Ministros aprobó el Real Decreto 523/2006, por el que se suprime la exigencia de aportar el certificado de empadronamiento, como documento probatorio del domicilio y residencia, en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes.

Los objetivos de dicha norma son, por un lado, no exigir a quien tenga la condición de interesado en los procedimientos cuya tramitación y resolución corresponda a la Administración General del Estado o a los organismos públicos vinculados o dependientes de aquélla, la aportación del certificado de empadronamiento como documento acreditativo del domicilio y residencia; y por otro sustituir, en los procedimientos para cuya tramitación sea imprescindible acreditar de modo fehaciente los datos del domicilio y residencia del interesado, la presentación de documento acreditativo por una consulta electrónica mediante un Sistema de Verificación de Datos de Residencia puesto a disposición de los organismos de la Administración General del Estado por parte del Ministerio de Administraciones Públicas y el Instituto Nacional de Estadística dependiente del Ministerio de Economía y Hacienda.

A partir de la puesta en producción de este sistema es el propio Departamento ante el que se solicita el trámite el encargado de comprobar, de oficio, la residencia del interesado. Esta consulta se realizará, en los casos en los que sea estrictamente necesario y tras obtener la autorización del interesado. La consulta se realizará con máximas garantías de seguridad y preservando la privacidad de los datos. En caso de que el interesado no dé su consentimiento a realizar esa consulta, deberá aportar el documento acreditativo de residencia que estime apropiado el organismo tramitador del expediente.

La presente Orden Ministerial tiene por objeto dar cumplimiento al mandato señalado en el Real Decreto 523/2006 de 28 de abril. A tal fin, se han tenido en consideración las

experiencias previas, las implicaciones técnicas, la búsqueda de racionalidad y sencillez de uso y el aprovechamiento de las ventajas de las economías de escala.

En su virtud, previo respectivos informes favorables del Consejo Superior de Administración Electrónica y de la Agencia Española de Protección de Datos, a propuesta de los Ministros de Economía y Hacienda y de Administraciones Públicas, dispongo:

**Artículo único.** *Objeto.*

1. Se aprueba el Reglamento Técnico del Sistema de Verificación de Datos de Residencia, que figura como anexo a la presente Orden Ministerial, como instrumento que establece la configuración, características, requisitos y procedimientos de acceso al citado Sistema.

2. Se fija como fecha de operatividad del Sistema de Verificación de Datos de Residencia la de entrada en vigor de la presente Orden, a partir de la cual no podrá exigirse en los procedimientos cuya tramitación y resolución corresponda a la Administración General del Estado, o a los Organismos vinculados o dependientes de aquélla, la aportación de certificados de empadronamiento, salvo en los supuestos previstos en el Real Decreto 523/2006, de 28 de abril.

3. La presente Orden Ministerial se aprueba en aplicación de lo dispuesto en la disposición final primera del Real Decreto 523/2006, de 28 de abril, por el que se suprime la exigencia de aportar el certificado de empadronamiento, como documento probatorio del domicilio y residencia, en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes. Lo dispuesto en esta Orden Ministerial se aplicará en todo caso de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa aplicable en esta materia.

**Disposición final primera.** *Aplicación y desarrollo.*

1. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio de Economía y Hacienda y previo informe del Consejo Superior de Administración Electrónica, se establecerán los parámetros de calidad de la prestación del servicio del Sistema de Verificación de Datos de Residencia y de cumplimiento de los requisitos y condiciones establecidas en la presente Orden Ministerial. A estos efectos, el Ministerio de Administraciones Públicas establecerá instrumentos de validación y vigilancia del cumplimiento de lo establecido en el párrafo anterior, sin perjuicio de las competencias de los Órganos de Control Interno.

2. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio de Economía y Hacienda y previo informe del Consejo Superior de Administración Electrónica, se podrá proceder a la actualización o modificación del Reglamento Técnico que se aprueba por la presente Orden Ministerial.

3. Se faculta a los Subsecretarios de los departamentos Ministeriales, a los Presidentes de los Organismos Públicos o a los responsables ministeriales correspondientes, para la adopción de las instrucciones o medidas que resulten adecuadas para garantizar el acceso y la utilización del Sistema de Verificación de Datos de Residencia por los órganos y unidades correspondientes a su ámbito.

**Disposición final segunda.** *Entrada en vigor.*

La presente Orden Ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

**ANEXO**

**Reglamento Técnico del Sistema de Verificación de Datos de Residencia**

Primero. Descripción del Sistema de Verificación de Datos de Residencia.

El Sistema de Verificación de Datos de Residencia puesto a disposición de los Departamentos y Organismos de la Administración General del Estado por parte del Ministerio de Administraciones Públicas se establece como servicio horizontal para la consulta y comprobación de los datos sobre residencia de los ciudadanos mediante el acceso a los Padrones municipales coordinados por el Instituto Nacional de Estadística, en base a lo dispuesto en la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local, en relación con el Padrón Municipal, en la que se atribuye al Instituto Nacional de Estadística, entre otras, la función de coordinación de los distintos padrones municipales. Ésta información se encuentra registrada y custodiada en los ficheros del Instituto Nacional de Estadística registrados en la Agencia de Protección de Datos con la denominación «PADRONES MUNICIPALES», conforme a la Orden ECO/143/2002, de 10 de enero, publicada en el BOE 26, de 30 de enero de 2002.

Segundo. Adopción de medidas de seguridad, organizativas o técnicas del acceso al Sistema de Verificación de Datos de Residencia.

1. Con carácter general los organismos que accedan al Sistema de Verificación de Datos de Residencia cumplirán con las medidas de seguridad, conservación y normalización que se detallan en los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades aprobados por el Consejo Superior de Administración Electrónica mediante Resolución de 26 de mayo de 2003 y revisiones posteriores.

2. El alcance e intensidad de aplicación de las medidas de seguridad, conservación y normalización vendrán determinadas por el resultado del análisis y gestión de riesgos que se realice, recomendándose a estos efectos la utilización de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) del Consejo Superior de Administración Electrónica.

3. Lo dispuesto en esta Orden Ministerial se aplicará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa aplicable en esta materia como el Reglamento de Medidas de Seguridad de los ficheros automatizados de datos de carácter personal aprobado por Real Decreto 994/1999, de 11 de junio.

Tercero. Acceso al Sistema de Verificación de Datos de Residencia.

1. El acceso al Sistema de Verificación de Datos de Residencia se realizará a través del Sistema de Aplicaciones y Redes para las Administraciones Públicas, siguiendo el esquema de conexión que ésta tiene establecido para cualquier departamento u organismo público. Sólo en casos debidamente justificados y previa aprobación, por parte de la Secretaría del Consejo Superior de Administración Electrónica, de un plan para la ordenación de las comunicaciones se habilitarán temporalmente mecanismos de conexión alternativos.

2. El Sistema de Verificación de Datos de Residencia presentará dos formas de acceso para realizar las correspondientes consultas sobre el lugar de domicilio y residencia de un ciudadano:

Un interfaz accesible a través de un navegador de Internet, conforme al RFC 2616: Protocolo de Transferencia de Hipertexto – HTTP/1.1 o superior, del IETF, donde un empleado público, debidamente acreditado e identificado, podrá realizar consultas con sólo disponer de un navegador con acceso al Sistema de Aplicaciones y Redes para las Administraciones Públicas y firma electrónica.

Un interfaz automatizado de servicio web, conforme al estándar WSDL 1.1 o superior del W3C cuya definición inicial, y sucesivas actualizaciones, serán puestas a disposición de los departamentos y organismos a través del Consejo Superior de Administración Electrónica y su Comisión Permanente.

Cuarto. Requisitos de autenticidad para el acceso al Sistema de Verificación de Datos de Residencia.

1. Los accesos al Sistema de Verificación de Datos de Residencia se efectuarán utilizando certificados electrónicos reconocidos.

2. Los certificados electrónicos que se utilicen para identificarse ante el Sistema de Verificación de Datos de Residencia deberán ser certificados reconocidos que cumpla la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 9594-8 de 1997).

3. No podrán utilizarse certificados electrónicos caducados o revocados para acceder al Sistema de Verificación de Datos de Residencia.

Quinto. Requisitos de confidencialidad del Sistema de Verificación de Datos de Residencia.

1. El Sistema de Verificación de Datos de Residencia, a partir del Número del Documento de Identificación del Ciudadano y/o de un conjunto de datos personales suficientes para identificar unívocamente al mismo, devolverá el total, o un subconjunto de los datos referentes al domicilio y residencia asociados a un ciudadano:

Provincia.
Municipio.
Entidad Colectiva.
Entidad Singular.
Núcleo.
Dirección (Via, Kmt, Número, Número Superior, Bloque, Portal, Escalera, Planta, Puerta).

El conjunto de datos a los que tenga acceso cada usuario del sistema será establecido, previa autorización y justificación, por parte del responsable en la Organización Administrativa.

En caso de que los datos introducidos no fueran suficientes para identificar de manera única a un ciudadano el sistema no devolverá en la respuesta información sobre ningún ciudadano.

2. Sólo organismos públicos debidamente autorizados tendrán acceso al Sistema de Verificación de Datos de Residencia. En todo organismo público existirá un responsable o administrador delegado del sistema que autorizará los accesos al Sistema de Verificación de Datos de Residencia.

3. Para realizar la consulta al Sistema de Verificación de Datos de Residencia, será preciso el consentimiento del interesado cuyos datos se vayan a consultar, salvo que una norma de rango de ley autorice dicha consulta. Dicho consentimiento deberá constar en la solicitud de iniciación del procedimiento, o en cualquier otra comunicación posterior, siempre y cuando dicha comunicación sea previa a la consulta en el sistema, no pudiendo realizarse consulta alguna en caso de no contar con el consentimiento de forma fehaciente. Los impresos o formularios electrónicos de solicitudes de iniciación de procedimientos administrativos deberán adecuarse para recoger dicho consentimiento.

4. La consulta y el acceso a la información proporcionada por el Sistema de Verificación de Datos de Residencia deberá realizarse con una finalidad concreta, que quedará recogida en el momento de la consulta.

Sexto. Requisitos de integridad de la información proporcionada por el Sistema de Verificación de Datos de Residencia.

Todas las consultas que se realicen al Sistema de Verificación de Datos de Residencia, así como las respuestas que devuelva el propio sistema, deberán haber sido firmadas electrónicamente. Esta firma electrónica tiene por objeto garantizar tanto la integridad de los datos intercambiados como la identidad de las partes que intervienen y el no repudio de la consulta.

De la misma forma, todas las consultas que el Sistema de Verificación de Datos de Residencia deba realizar al Instituto Nacional de Estadística o a otros organismos con capacidad de informar sobre la residencia de los ciudadanos, así cómo las correspondientes respuestas obtenidas resultado de las mismas, habrán de ser debidamente firmadas electrónicamente para garantizar tanto la integridad de la información como la identidad de ambos organismos.

Séptimo. Requisitos de disponibilidad de la información proporcionada por el Sistema de Verificación de Datos de Residencia.

El Sistema de Verificación de Datos de Residencia estará disponible los 7 días de la semana las 24 horas del día.

Octavo. Garantías jurídicas del Sistema de Verificación de Datos de Residencia ante posibles recursos.

1. El servicio web proporcionado por este sistema sigue el estándar de intercambio de datos definido por la iniciativa «Sustitución de Certificados en Soporte Papel» del Consejo Superior de Administración Electrónica, que reúne, en base a la normativa vigente, las garantías jurídicas aplicables al intercambio de datos entre Administraciones Públicas.

2. El Sistema de Verificación de Datos de Residencia dispondrá de un módulo de auditoría, en el que quedarán registradas todas las consultas de datos de residencia realizadas, información de contexto asociada, la identidad del solicitante, la fecha y la finalidad de la consulta, y aquellos eventos relevantes desencadenados a partir de la propia consulta. Se garantizará la integridad y no repudio de la información registrada mediante técnicas de firma electrónica y sellado de tiempo, estableciéndose, asimismo, medidas técnicas para garantizar la disponibilidad y recuperación de aquella información que no se mantenga on-line por motivos de eficiencia técnica o seguridad.

3. Para certificar la fecha y tiempo de las actividades y sucesos registrados en el Sistema de Verificación de Datos de Residencia se hará uso del Servicio de Sellado de Tiempo de la Plataforma de Firma Electrónica del Ministerio de Administraciones Públicas, sincronizada con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara el Laboratorio de la Armada como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

4. Sólo personal de la Administración Pública debidamente autorizado y acreditado podrá acceder a las funcionalidades de auditoria del Sistema de Verificación de Datos de Residencia.

Noveno. Condiciones de la prestación del servicio.

1. La gestión del Sistema de Verificación de Datos de Residencia corresponde al Ministerio de Administraciones Públicas.

2. Los organismos públicos que hagan uso de este servicio estarán sujetos a las medidas de seguridad, los requisitos de autenticidad, integridad, confidencialidad, disponibilidad y criterios técnicos establecidos en esta Orden Ministerial.

3. Para poder acceder al Sistema de Verificación de Datos de Residencia, los Organismos Administrativos deberán designar a un responsable, tal y como se indica en el apartado segundo del punto quinto del presente anexo técnico, que será el encargado de autorizar los accesos en su organismo. El nombramiento y cese de este responsable deberá ser comunicado al Ministerio de Administraciones Públicas, para la asignación de los permisos adecuados de acceso al sistema o la cancelación de los mismos.

# § 44

## Orden HAP/1949/2014, de 13 de octubre, por la que se regula el Punto de Acceso General de la Administración General del Estado y se crea su sede electrónica

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 260, de 27 de octubre de 2014
Última modificación: 26 de noviembre de 2015
Referencia: BOE-A-2014-10908

En el marco de las reformas estructurales iniciadas por el Gobierno de la Nación, el pasado 26 de octubre de 2012 se acordó por el Consejo de Ministros la creación de una Comisión para la Reforma de las Administraciones Públicas (CORA) con el expreso objeto de realizar un estudio integral de la situación de las Administraciones Públicas en España y de proponer las reformas que sería necesario introducir en las mismas para dotarlas del tamaño, la eficiencia y la flexibilidad demandadas por los ciudadanos y la economía del país, y para transformar su estructura con vistas a posibilitar el crecimiento económico, la prestación efectiva de los servicios públicos y eliminar aquellas disfuncionalidades y defectos que pudieran dificultar ambos.

Entre otras medidas de reforma, CORA ha propuesto al Gobierno el establecimiento del Punto de Acceso General (PAG) como punto de entrada general, vía Internet, del ciudadano a las Administraciones Públicas. El fundamento de esta medida es la constatación de que en el momento actual existe una gran dispersión de la información de las Administraciones en distintos portales y páginas web, que provoca dificultades en el acceso de los ciudadanos a los procedimientos y servicios administrativos, informaciones duplicadas y falta de una coordinación adecuada en todas estas materias.

El PAG dispone de cobertura normativa en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, cuyo artículo 8 apartado 2, determina que la Administración General del Estado (AGE) contará con un sistema de varios canales o medios para garantizar a todos los ciudadanos la prestación de servicios electrónicos. Y en la letra b) de dicho apartado señala expresamente que, entre los puntos de acceso electrónico, se creará un Punto de Acceso General a través del cual, los ciudadanos puedan, en sus relaciones con la Administración General del Estado y sus Organismos Públicos, acceder a toda la información y a los servicios disponibles.

Por su parte, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, tanto en su preámbulo, como en sus artículos 7, 8, 9, 24 y 31, define las características básicas que deberá tener el Punto y señala que habrá de contener la sede electrónica que, en este ámbito, facilita el acceso a los servicios, procedimientos e informaciones accesibles de la Administración General del Estado y de los organismos públicos vinculados o dependientes de la misma.

Las funciones principales del citado Punto, como posibilitar el acceso a la información y servicios de la Administración General del Estado, Comunidades Autónomas y Entidades

Locales, han venido realizándose parcialmente en los últimos años a través del sitio web Portal 060 (www.060.es), establecido en el ámbito de la Red 060 de Atención al Ciudadano, creada al amparo del Acuerdo de Consejo de Ministros de 15 julio de 2005 y, por ende, establecida con anterioridad a la propia ley 11/2007, de 22 de junio.

En ejecución de esta medida, y de las disposiciones normativas de la Ley 11/2007, de 22 de junio, y su Real Decreto de desarrollo, se dicta la presente orden, que tiene por finalidad la creación del PAG, la definición de su contenido y de su régimen de gobernanza y gestión, así como la creación de un fichero de datos de acuerdo con las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Adicionalmente, esta orden se dirige a crear la sede electrónica del PAG, en cumplimiento de las previsiones del Real Decreto 1671/2009, de 6 de noviembre.

La citada ley 11/2007, de 22 junio, estableció el concepto de sede electrónica, que define en el artículo 10, apartado 1, como aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias, señalando en el número 3 del mismo precepto que cada Administración Pública determinará las condiciones e instrumentos de creación de sus sedes electrónicas.

Por su parte, el Real Decreto 1671/2009, de 6 de noviembre, determina específicamente en su Título II, que las sedes electrónicas se crearán mediante orden del Ministro correspondiente o resolución del titular del organismo público, que deberá publicarse en el «Boletín Oficial del Estado», señalando el contenido mínimo de la misma.

La presente orden ha sido sometida al previo informe de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37, párrafo h), de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y ha sido informada por la Comisión Permanente del Consejo Superior de Administración Electrónica.

En su virtud, a propuesta del Ministro de Hacienda y Administraciones Públicas, dispongo:

## CAPÍTULO I

## Disposiciones generales

**Artículo 1.** *Objeto.*

La presente orden tiene por objeto la regulación del Punto de Acceso General (en adelante PAG) y de su sede electrónica, así como la regulación del fichero de datos de carácter personal de la misma.

## CAPÍTULO II

## Punto de Acceso General

**Artículo 2.** *Alcance y características.*

1. El PAG, con los dominios www.administracion.es y www.administracion.gob.es, ofrecerá a los ciudadanos y empresas la información sobre los procedimientos y servicios de los Departamentos ministeriales y de los Organismos públicos vinculados o dependientes y reunirá la información de la actividad y la organización de las Administraciones Públicas.

2. El PAG contiene además el acceso a la sede electrónica asociada al mismo, de acuerdo con las características previstas en el artículo 7.

A este efecto, los Departamentos ministeriales y los Organismos públicos vinculados o dependientes deberán coordinar sus sedes electrónicas con la sede del PAG en los términos previstos en el artículo 5.

3. El PAG proporcionará información sobre los procedimientos y servicios correspondientes a otras Administraciones Públicas, mediante la formalización de los correspondientes instrumentos de colaboración.

4. Sin perjuicio de estos instrumentos, el acceso a procedimientos, servicios, e informaciones de las Administraciones Públicas, así como el intercambio de información entre ellas, se ajustará a lo previsto en los artículos 8 y 9 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

5. Respecto a la coordinación del PAG con los portales electrónicos de los organismos internacionales y de las Administraciones Públicas extranjeras, especialmente de la Unión Europea y sus Estados miembros, se estará a lo dispuesto en la normativa correspondiente o a los convenios y acuerdos que pudieran existir. Las actuaciones de coordinación con los portales de la Unión Europea se canalizarán a través de la Representación Permanente de España en la misma.

**Artículo 3.** *Contenido y funcionalidades.*

1. El PAG deberá garantizar, de forma gradual y progresiva a medida que los recursos y desarrollos técnicos lo permitan, el acceso a los siguientes servicios:

a) Los portales de los Departamentos ministeriales y Organismos públicos vinculados o dependientes.

b) Su sede electrónica y las sedes electrónicas de los Departamentos ministeriales y de los Organismos públicos vinculados o dependientes.

c) Los servicios que la Administración pone a disposición de los ciudadanos y especialmente, los más usados por los ciudadanos.

d) Portal de transparencia.

e) Otros portales destacados de ámbito estatal como el portal de Datos abiertos, la Ventanilla Única de la Directiva de Servicios y aquellos de similar naturaleza.

f) Las áreas restringidas o privadas para los usuarios.

2. Además, el PAG contendrá información administrativa de carácter horizontal de los Departamentos ministeriales y Organismos públicos, vinculados o dependientes como las ayudas, becas, subvenciones, empleo público y legislación, que sean de interés para el ciudadano.

3. El PAG tendrá un espacio dedicado a la participación ciudadana y posibilitará la interactuación del ciudadano a través de las redes sociales más extendidas. También dispondrá de los mecanismos precisos que faciliten el acceso de sus contenidos a los diferentes dispositivos móviles existentes, a medida que los recursos y desarrollos técnicos lo permitan.

**Artículo 4.** *Acceso.*

Serán canales de acceso a los servicios del PAG:

1. Para el acceso electrónico, Internet, con las características definidas en el artículo 2.

2. Para la atención presencial, la oficina 060 de calle María de Molina, 50 (Madrid), así como las Oficinas 060 de Delegaciones y Subdelegaciones del Gobierno y de Direcciones Insulares, conforme a las competencias definidas en las normas reguladoras de la organización ministerial y el resto de las oficinas de las Administraciones Públicas en el marco de los convenios suscritos o que pudieran suscribirse, sin perjuicio del acceso a través de los registros regulados en el artículo 38 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Para la atención telefónica, los servicios de información departamental, en el teléfono 060.

**Artículo 5.** *Titularidad y gestión.*

1. De acuerdo con lo regulado en el Real Decreto 1671/2009, de 6 de noviembre, la titularidad del PAG corresponderá al Ministerio de Hacienda y Administraciones Públicas, que establecerá los principios generales y directrices básicos de funcionamiento del mismo.

2. La gestión del PAG corresponde a la Dirección General de Organización Administrativa y Procedimientos que la ejercerá a través de la Subdirección General de la

Inspección General de Servicios de la Administración General del Estado y Atención al Ciudadano, en coordinación con la Dirección de Tecnologías de la Información y las Comunicaciones, de acuerdo con lo previsto en el artículo 16.1.e) del Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas.

3. Cada Departamento ministerial u Organismo público se responsabilizará de la provisión y actualización de la información que provea el portal en relación a sus procedimientos, servicios e informaciones a través de los mecanismos que se establezcan.

**Artículo 6.** *Gobernanza.*

1. Con el fin de garantizar una adecuada coordinación de la información contenida en el PAG y asegurar los necesarios niveles de colaboración para posibilitar la actualización permanente de la información y su adecuación a las demandas de los ciudadanos, se crea un Grupo de Trabajo, de acuerdo con lo dispuesto en el artículo 40.3 de la Ley 6/1997, de 14 de noviembre, de Organización y Funcionamiento de la Administración General del Estado, adscrito a la Dirección General de Organización Administrativa y Procedimientos. Este grupo contará con un representante de la Dirección de Tecnologías de la Información y las Comunicaciones así como con un representante por cada Departamento ministerial, al menos de nivel 30, que serán designados por la Subsecretaría de cada Departamento y que asumirán la representación de los Organismos públicos vinculados o dependientes del mismo.

2. Dicho Grupo de Trabajo tendrá atribuidas las siguientes funciones:

a) Potenciar la colaboración entre las unidades de información administrativa y/o unidades de gestión de sitios web de los distintos Departamentos ministeriales y de los Organismos públicos vinculados o dependientes a efectos de la actualización de la información contenida en el PAG.

b) Analizar los modelos de gobernanza que posibiliten una adecuada gestión y mantenimiento de la información.

c) Facilitar la coordinación y corresponsabilidad de los Departamentos ministeriales y de los Organismos públicos vinculados o dependientes respecto a la información contenida en el PAG.

d) Garantizar las acciones que se consideren convenientes para ofrecer un buen servicio de información administrativa y disponer de la información interdepartamental y de la que ofrezca cada Departamento ministerial y Organismo público vinculado o dependiente.

e) Colaborar en la gestión de la sede electrónica regulada en el Capítulo III de la presente orden.

3. Cada Departamento ministerial y Organismo público vinculado o dependiente a su vez se dotará de la estructura organizativa necesaria para garantizar la adecuada coordinación interna con el objeto de proveer los contenidos y sus actualizaciones en el PAG.

4. Sin perjuicio de lo establecido en su caso en los correspondientes instrumentos de colaboración, la participación y seguimiento de los contenidos del PAG referentes a otras Administraciones Públicas se verificarán a través del Comité Sectorial de Administración Electrónica.

## CAPÍTULO III

## Sede Electrónica del PAG

**Artículo 7.** *Creación y ámbito de aplicación.*

1. Se crea la sede electrónica del PAG, de acuerdo con lo dispuesto en los artículos 3 y 9 del Real Decreto 1671/2009, de 6 de noviembre.

2. El ámbito de aplicación de la sede comprenderá la totalidad de los Departamentos ministeriales y de los Organismos públicos vinculados o dependientes. Asimismo, la sede electrónica del PAG extenderá su ámbito a los organismos que se determinen en los instrumentos de colaboración con otras Administraciones Públicas que, en su caso, formalice

el Ministerio de Hacienda y Administraciones Públicas, al amparo de lo establecido en los artículos 3.3 y 9.1 del Real Decreto 1671/2009, de 6 de noviembre.

3. Esta sede se considerará como la sede central de la Administración General del Estado.

**Artículo 8.** *Características.*

1. A través de la sede electrónica del PAG se podrá acceder a los procedimientos y servicios que requieran la autenticación de los ciudadanos o de la Administración Pública en sus relaciones con éstos por medios electrónicos, así como aquellos otros respecto a los que se decida su inclusión en la sede por razones de eficacia y calidad en la prestación de servicios a los ciudadanos y que estén accesibles en las sedes electrónicas de los órganos correspondientes. A medida que los recursos y desarrollos técnicos lo permitan, este acceso se podrá realizar sin tener que identificarse de nuevo.

2. La dirección electrónica de referencia de la sede será:

https://sede.administracion.gob.es.

3. Los servicios incluidos en la sede electrónica del PAG cumplirán los principios de accesibilidad y usabilidad, establecidos en la Ley 11/2007, de 22 de junio, así como en los términos dictados por la normativa vigente en esta materia en cada momento.

4. Los contenidos publicados en la sede electrónica del PAG responderán a los criterios de seguridad e interoperabilidad según lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y por el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

5. Serán canales de acceso a los servicios disponibles en la sede:

a) Para el acceso electrónico, Internet, con las características definidas en el presente artículo.

b) Para la atención presencial, la oficina 060 de calle María de Molina, 50 (Madrid), así como las Oficinas 060 de Delegaciones y Subdelegaciones del Gobierno y de Direcciones Insulares, conforme a las competencias definidas en las normas reguladoras de la organización ministerial, sin perjuicio del acceso a través de los registros regulados en el artículo 38 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

c) Para la atención telefónica, los servicios de información departamental, en el teléfono 060.

**Artículo 9.** *Contenidos.*

1. La sede electrónica del PAG dispondrá del contenido mínimo y de los servicios previstos expresamente en los apartados 1 y 2 del artículo 6 del Real Decreto 1671/2009, de 6 de noviembre.

2. Además la sede electrónica del PAG dispondrá de los siguientes contenidos específicos:

a) Acceso a Trámites y Servicios en línea disponibles en las sedes electrónicas.
b) Registro Electrónico Común.
c) Dirección Electrónica Habilitada.
d) Registro Electrónico de Apoderamientos.
e) Registro de Funcionarios Habilitados.
f) Servicios que requieran de autenticación de la administración y/o del ciudadano como la inscripción en pruebas selectivas, cambio de domicilio y notificaciones electrónicas, entre otros.
g) Enlace a la orden de creación, publicada en el Boletín Oficial del Estado.
h) Buzón de contacto del PAG.
i) Cualquier otro contenido de interés para el ciudadano que deba figurar en la Sede Electrónica del PAG.

3. A medida que los recursos y desarrollos técnicos lo permitan, la Sede Electrónica del PAG posibilitará el acceso a sus contenidos en lenguas cooficiales.

**Artículo 10.** *Titularidad y gestión de la sede electrónica del PAG.*

1. La titularidad de la Sede Electrónica del PAG corresponderá al Ministerio de Hacienda y Administraciones Públicas en los mismos términos previstos en el artículo 5.1.

2. La gestión de la sede corresponde a la Dirección General de Organización Administrativa y Procedimientos que la ejercerá a través de la Subdirección General de la Inspección General de Servicios de la Administración General del Estado y Atención al Ciudadano, en coordinación con la Dirección de Tecnologías de la Información y las Comunicaciones, de acuerdo con lo previsto en el artículo 16.1 e) del Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas.

3. Los Departamentos ministeriales y los Organismos públicos vinculados o dependientes de los mismos participarán en la gestión de la sede electrónica del PAG a través del mecanismo previsto en el artículo 6.

4. Sin perjuicio de lo establecido en su caso en los correspondientes instrumentos de colaboración, la participación y seguimiento de los contenidos de la sede electrónica del PAG referentes a otras Administraciones Públicas, se verificarán a través del Comité Sectorial de Administración Electrónica.

5. El titular de la sede electrónica del PAG será responsable de la integridad, veracidad y actualización de la información y servicios a los que pueda accederse a través de la misma. En el caso de los enlaces o vínculos cuya responsabilidad corresponde a distinto órgano o Administración Pública, el titular de la sede electrónica del PAG no será responsable de la integridad, veracidad ni actualización de aquéllos.

**Artículo 11.** *Medios para la formulación de quejas y sugerencias.*

1. Los medios disponibles para la formulación de quejas y sugerencias en relación con el contenido, gestión y servicios ofrecidos en la sede que se crea en la presente orden y sin perjuicio de los procedimientos específicos, serán los siguientes:

a) Presentación presencial o por correo postal ante los registros y las oficinas de atención al público de los servicios centrales y de las oficinas periféricas del Ministerio de Hacienda y Administraciones Públicas, así como en los lugares previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común, dirigidas a los órganos u organismos responsables, y de acuerdo con lo dispuesto en el artículo 9 y según el procedimiento establecido en capítulo IV del Real Decreto 951/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

b) Presentación electrónica a través del Servicio electrónico de quejas y sugerencias de la Inspección General del Ministerio de Hacienda y Administraciones Públicas, enlazado en la Sede electrónica del PAG así como de aquellos medios que prevé la Ley 11/2007, de 22 de junio.

2. No se considerarán medios para la formulación de quejas y sugerencias los servicios de asesoramiento electrónico al usuario para la correcta utilización de la sede, sin perjuicio de su obligación, cuando existan, de atender las cuestiones que susciten los ciudadanos.

**Disposición adicional primera.** *Régimen económico.*

Las medidas contenidas en esta orden se cumplirán con los medios presupuestarios, personales y materiales existentes en cada Departamento ministerial u Organismo público vinculado o dependiente responsable de la información que provea el PAG y en ningún caso podrá generar incremento de gasto público.

**Disposición adicional segunda.** *Referencias al portal 060.*

Las referencias al portal 060 que se contengan en cualquier Convenio de colaboración suscrito para la implantación de oficinas integradas se entenderán realizadas al PAG.

**Disposición transitoria única.** *Portal 060 y Sede 060.*

El portal 060 (www.060.es) y su sede (https://sede.060.gob.es) seguirán en funcionamiento hasta la puesta en marcha del PAG.

**Disposición final primera.** *Desarrollo.*

Se autoriza al Secretario de Estado de Administraciones Públicas a dictar las instrucciones precisas para el cumplimiento de la presente orden.

**Disposición final segunda.** *Modificación de la Orden HAP 2478/2013, de 20 de diciembre, por la que se regulan los ficheros de datos de carácter personal existentes en el departamento y en determinados organismos adscritos al mismo.*

1. En cumplimiento de lo previsto en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, se crea el fichero de datos personales «Sede electrónica del Punto de Acceso General», cuya titularidad corresponde a la Dirección General de Organización Administrativa y Procedimientos, situada en calle María de Molina, número 50, 28071, Madrid, válido a efectos del ejercicio por parte de los ciudadanos de los derechos previstos por dicha ley.

2. El contenido del fichero se recoge en el anexo de la presente orden.

3. Dicho fichero se añade a los ficheros de la Dirección General de Organización Administrativa y Procedimientos del Ministerio de Hacienda y Administraciones Públicas que se recogen en la Orden ministerial HAP 2478/2013, de 20 de diciembre, por la que se regulan los ficheros de datos de carácter personal existentes en el departamento y en determinados organismos públicos adscritos al mismo.

**Disposición final tercera.** *Entrada en vigor.*

La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

**ANEXO**

**Fichero de datos personales**

**(Suprimido)**

# § 45

## Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre

Ministerio de la Presidencia
«BOE» núm. 88, de 12 de abril de 2010
Última modificación: sin modificaciones
Referencia: BOE-A-2010-5788

Una de las manifestaciones más relevantes de la Administración electrónica es la práctica de notificaciones por medios electrónicos, informáticos y telemáticos por las distintas Administraciones Públicas. Esta posibilidad, vislumbrada en el artículo 70 de la Ley 30/1992, cobró carta de naturaleza específica cuando la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, incorporo sendos textos de idéntico tenor en los artículos 105 de la Ley General Tributaria y 59 de la Ley 30/1992, configurando un nuevo modelo de notificación mediante la puesta a disposición de la actuación correspondiente de manera que los efectos de la notificación se producen bien por el acceso a su contenido bien por el simple transcurso del lapso de diez días desde la puesta a disposición sin que tenga lugar dicho acceso por parte del destinatario. El Real Decreto 209/2003, de 21 de febrero, desarrolla esta última previsión, siendo su disposición final primera desarrollada a su vez por la Orden PRE/1551/2003, de 10 de junio, con el objeto de establecer los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse y las condiciones que han de reunir el órgano, organismo o entidad habilitada para la prestación del servicio de dirección electrónica única así como las condiciones de su prestación. Toda la regulación de la notificación electrónica se fundamenta en la existencia de una única dirección electrónica a tal efecto en el ámbito de la Administración del Estado y en su carácter voluntario.

La Ley 11/2007, de 11 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, regula de modo similar la notificación por medios electrónicos, admitiendo que en determinados supuestos pueda establecerse esta notificación con carácter obligatorio. El reciente Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, desarrolla en su artículo 38 la notificación mediante la puesta a disposición del documento electrónico a través de dirección electrónica habilitada, previendo que bajo responsabilidad del Ministerio de la Presidencia existirá un sistema de dirección electrónica habilitada para la práctica de estas notificaciones que quedará a disposición de todos los órganos y organismos públicos vinculados o dependientes de la Administración General del Estado que no establezcan sistemas de notificación propios. Además, en su apartado segundo se establece que «Cuando se establezca la práctica de notificaciones electrónicas con carácter obligatorio, la dirección electrónica habilitada a que se refiere el apartado anterior será asignada de oficio y podrá tener vigencia indefinida, conforme al régimen que

se establezca por la orden del Ministro de la Presidencia a la que se refiere la disposición final primera».

En su virtud, previo informe del Consejo Superior de Administración Electrónica, dispongo:

**Artículo 1.** *Objeto.*

La presente Orden tiene por objeto establecer el régimen de un sistema de notificación mediante dirección electrónica habilitada, a disposición de los órganos y organismos vinculados o dependientes de la Administración General del Estado que no establezcan sistemas de notificación propios, tanto en los casos de notificación voluntaria como cuando tenga carácter obligatorio, de acuerdo con lo previsto en el artículo 38 y en la disposición final primera del Real Decreto 1671/2009, de 8 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

**Artículo 2.** *Dirección electrónica habilitada responsabilidad del Ministerio de la Presidencia.*

1. La titularidad de la dirección electrónica a partir de la cual se construyan las direcciones electrónicas habilitadas de los interesados, corresponde al Ministerio de la Presidencia.

2. La prestación del servicio de dirección electrónica habilitada se llevará a cabo por el Ministerio de la Presidencia, directamente, o a través del prestador que se establezca conforme a lo dispuesto en el ordenamiento jurídico.

3. El directorio del servicio de dirección electrónica habilitada deberá recoger el nombre y apellidos o la razón o denominación social del interesado, el número de identificación fiscal y la dirección electrónica habilitada.

4. El sistema de dirección electrónica habilitada se sujetará a lo establecido en los Esquemas Nacionales de Interoperabilidad y de Seguridad, así como a la normativa protectora en materia de datos de carácter personal.

**Artículo 3.** *Asignación de dirección electrónica habilitada.*

1. Se asignará una dirección electrónica habilitada, con la inclusión en el correspondiente directorio, cuando el interesado solicite su apertura.

2. Asimismo se asignará en todo caso de oficio una dirección electrónica cuando se reciba de un órgano u organismo de la Administración General del Estado el aviso para la práctica de una notificación conforme al sistema establecido en la presente Orden.

**Artículo 4.** *Vigencia.*

1. La dirección electrónica habilitada tendrá vigencia indefinida, excepto en los supuestos en que se solicite su revocación por el titular, por fallecimiento de la persona física o extinción de la personalidad jurídica, que una resolución administrativa o judicial así lo ordene o por el transcurso de tres años sin que se utilice para la práctica de notificaciones, supuesto en el cual se inhabilitará esta dirección electrónica, comunicándose así al interesado.

2. No obstante, no se inhabilitará esta dirección electrónica cuando se establezca la práctica de notificaciones electrónicas con carácter obligatorio, y así se confirme por los órganos u organismos afectados al prestador del servicio de dirección electrónica.

**Artículo 5.** *Autenticación.*

1. La identificación y autenticación de la notificación se hará por alguno de los medios admitidos conforme a la ley 11/2007 y de acuerdo con lo establecido por el Real Decreto 1671/2009.

2. La autenticación de los ciudadanos en el acceso al contenido del documento notificado se hará mediante certificados electrónicos que se admitan conforme a lo establecido en la normativa vigente.

3. En particular, las personas jurídicas y entidades sin personalidad podrán acceder al contenido del documento notificado mediante los certificados electrónicos que se admitan.

**Artículo 6.** *Confidencialidad.*

1. El sistema de notificación electrónica contendrá mecanismos de cifrado para proteger la confidencialidad de los datos en las transmisiones.

2. Asimismo, el sistema contará con las medidas de seguridad adecuadas para que el prestador del servicio de dirección electrónica habilitada no acceda al contenido de los actos y actuaciones administrativas que se notifiquen.

**Artículo 7.** *Referencia temporal.*

1. El sistema de notificación electrónica acreditará las fechas y horas en que se produzca la puesta a disposición del interesado del acto objeto de notificación. Ello tendrá lugar mediante la recepción en la dirección electrónica asignada al destinatario del aviso de la puesta a disposición de la notificación, incluyendo el propio documento que se notifica o, al menos, su huella electrónica.

Para la referencia temporal de los actos y certificaciones se utilizará una marca de tiempo entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora. La fecha y hora utilizada se sincronizará con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara el Laboratorio del Real Instituto y Observatorio de la Armada como laboratorio depositario del patrón Nacional de Tiempo y laboratorio asociado al Centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

La información relativa a las marcas de tiempo se asociará en la forma que determine el Esquema Nacional de Interoperabilidad.

2. El sistema de dirección electrónica habilitada acreditará igualmente el acceso del destinatario al contenido del documento notificado, así como cualquier causa técnica que imposibilite alguna de las circunstancias de este artículo.

**Artículo 8.** *Seguridad.*

1. Los órganos de la Administración General del Estado y los organismos públicos vinculados o dependientes de aquélla que pongan en marcha dispositivos y aplicaciones de registro y notificación deben adoptar medidas de seguridad para la salvaguarda de la confidencialidad. En cualquier caso establecerán las siguientes medidas:

a) Medidas de seguridad física.

b) Control de los accesos a los dispositivos y aplicaciones de registro y notificación, en especial los que lleguen a través de las redes de comunicaciones.

c) Protección de los soportes de información y copias de respaldo.

d) Cifrado de las notificaciones, cuando así se establezca por la legislación sobre protección de los datos de carácter personal o lo estime necesario el órgano u organismo notificador.

2. El prestador del servicio de dirección electrónica única designará a un responsable de la seguridad, que se encargará de la realización y actualización del análisis y gestión de riesgos, del registro de incidencias de seguridad, de la correcta implementación de las salvaguardas de seguridad técnicas, organizativas, y de cuantas otras actuaciones en materia de seguridad sean necesarias para la protección de los sistemas a su cargo.

**Artículo 9.** *Disponibilidad.*

1. El sistema de dirección electrónica habilitada posibilitará el acceso permanente de los interesados a la dirección electrónica correspondiente, tanto para solicitar la asignación de una dirección electrónica habilitada como para acceder al contenido de las notificaciones puestas a su disposición.

2. El acceso se producirá a través del Punto de Acceso General de la Administración General del Estado, así como de las sedes electrónicas del Ministerio de la Presidencia y de

los órganos u organismos adheridos al sistema o, en su caso, del prestador del servicio de dirección electrónica.

3. Los órganos y organismos a los que se refiere el artículo anterior adoptarán las medidas organizativas y técnicas para garantizar la disponibilidad del servicio 7 días a la semana y 24 horas al día, y en cualquier caso las siguientes:

a) Adopción de medidas de protección frente a código dañino en los servidores de aplicación y en los soportes circulantes.

b) Preparación y mantenimiento operativo de un plan de contingencia.

**Artículo 10.** *Condiciones de prestación del servicio.*

1. El órgano, organismo o entidad al que, en su caso, corresponda la prestación del sistema de dirección electrónica habilitada, llevará a cabo las siguientes funciones:

a) Crear y mantener el directorio de direcciones electrónica habilitadas con la información proporcionada por los interesados.

b) Almacenar y custodiar los avisos de puesta a disposición en la dirección electrónica habilitada.

c) Gestionar los acuses de recibo de los interesados y de los órganos u organismos notificadores.

d) Mantener el registro de eventos de las notificaciones, el cual contendrá, al menos, la dirección electrónica, la traza de la fecha y la hora de la recepción de la puesta a disposición en la dirección electrónica y del acceso del interesado a la notificación y la descripción del contenido de la notificación.

e) Impedir el acceso al contenido de las notificaciones que se entienden rechazadas por el transcurso de diez días desde su puesta a disposición.

f) Establecer las medidas organizativas y técnicas para que la disponibilidad del servicio sea de siete días a la semana y veinticuatro horas al día.

g) Potestativamente, otras funciones de mejora del servicio y complementarias de las expresadas, como es el caso de aviso de puesta a disposición de los interesados de las notificaciones mediante mensajería o de cualquier otro modo.

2. El prestador del servicio de dirección electrónica habilitada deberá remitir al órgano u organismo actuante por cada notificación electrónica:

a) Certificación electrónica de la fecha y hora en la que recibe el aviso de puesta a disposición enviada por el órgano u organismo notificador.

b) Certificación electrónica de la fecha y hora en la que se produce la recepción en la dirección electrónica asignada al destinatario del aviso de la puesta a disposición de la notificación, incluyendo el propio acto o actuación notificada o, al menos, su sello electrónico.

c) Certificación electrónica en la que conste la fecha y hora en la que se produce el acceso del interesado al contenido de la notificación en la dirección electrónica.

d) Certificación electrónica del transcurso del plazo de diez días desde la puesta a disposición sin que se haya producido el acceso del interesado al contenido de la notificación en la dirección electrónica.

e) Certificación electrónica de cualquier incidencia que se produzca en la práctica de lo dispuesto en los apartados anteriores.

3. En el caso de cese de actividad o cambio del prestador del servicio de dirección electrónica, las bases de datos, los programas informáticos asociados, el registro de eventos y el dominio de direcciones electrónicas con las notificaciones que existan en ese momento y la documentación técnica, deberán entregarse al Ministerio de la Presidencia, o a la entidad que éste designe debidamente actualizadas.

4. Los programas necesarios para el correcto funcionamiento del sistema de notificación serán suministrados a los órganos y organismos notificadores por el prestador del servicio de dirección electrónica habilitada.

**Disposición transitoria única.** *Mantenimiento de la prestación del servicio.*

1. A la entrada en vigor de la presente Orden, la prestación del servicio de dirección habilitada seguirá realizándose a través de los servicios autorizados, de conformidad con la Orden PRE/1551/2003, de 10 de junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por la que se regula los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

2. En el plazo de tres meses desde la entrada en vigor de la presente Orden se llevarán a cabo las adaptaciones requeridas en la prestación del servicio de dirección habilitada.

**Disposición derogatoria única.** *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en esta Orden, y, especialmente, la Orden PRE/1551/2003, de 10 de junio, que desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, que regula los registros y notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de certificados por los ciudadanos.

**Disposición final.** *Entrada en vigor.*

La presente orden entrará en vigor al día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 5 de abril de 2010.–La Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, María Teresa Fernández de la Vega Sanz.

# § 46

# Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

Jefatura del Estado
«BOE» núm. 298, de 12 de noviembre de 2020
Última modificación: 9 de mayo de 2023
Referencia: BOE-A-2020-14046

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

## PREÁMBULO

### I

Desde el 1 de julio de 2016 es de aplicación el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, que supuso la transposición al ordenamiento jurídico español de la derogada Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, se encuentra desde entonces jurídicamente desplazada en todo aquello regulado por el citado Reglamento. El objeto de esta Ley es, por tanto, adaptar nuestro ordenamiento jurídico al marco regulatorio de la Unión Europea, evitando así la existencia de vacíos normativos susceptibles de dar lugar a situaciones de inseguridad jurídica en la prestación de servicios electrónicos de confianza.

La presente Ley no realiza una regulación sistemática de los servicios electrónicos de confianza, que ya han sido legislados por el Reglamento (UE) 910/2014, el cual, por respeto al principio de primacía del Derecho de la Unión Europea, no debe reproducirse total o parcialmente. La función de esta Ley es complementarlo en aquellos aspectos concretos que el Reglamento no ha armonizado y cuyo desarrollo prevé en los ordenamientos de los diferentes Estados miembros, cuyas disposiciones han de ser interpretadas de acuerdo con él.

II

En lugar de una revisión de la Directiva 1999/93/CE, la elección de un reglamento como instrumento legislativo por el legislador europeo, de aplicación directa en los Estados miembros, vino motivada por la necesidad de reforzar la seguridad jurídica en el seno de la Unión, terminando con la dispersión normativa provocada por las transposiciones de la citada Directiva en los ordenamientos jurídicos internos a través de leyes nacionales, que había provocado una importante fragmentación e imposibilitado la prestación de servicios transfronterizos en el mercado interior, agravada por las diferencias en los sistemas de supervisión aplicados en cada Estado miembro.

Así, mediante el Reglamento (UE) 910/2014 se persigue regular en un mismo instrumento normativo de aplicación directa en los Estados miembros dos realidades, la identificación y los servicios de confianza electrónicos en sentido amplio, armonizando y facilitando el uso transfronterizo de los servicios en línea, públicos y privados, así como el comercio electrónico en la UE, contribuyendo así al desarrollo del mercado único digital.

Por una parte, en el ámbito de la identificación electrónica, el Reglamento instaura la aceptación mutua, para el acceso a los servicios públicos en línea, de los sistemas nacionales de identificación electrónica que hayan sido notificados a la Comisión Europea por parte de los Estados miembros, con objeto de facilitar la interacción telemática segura con las Administraciones públicas y su utilización para la realización de trámites transfronterizos, eliminando esta barrera electrónica que excluía a los ciudadanos del pleno disfrute de los beneficios del mercado interior.

Por otra parte, introduce la regulación armónica de nuevos servicios electrónicos cualificados de confianza, adicionales a la tradicional firma electrónica, tales como el sello electrónico de persona jurídica, el servicio de validación de firmas y sellos cualificados, el servicio de conservación de firmas y sellos cualificados, el servicio de sellado electrónico de tiempo, el servicio de entrega electrónica certificada y el servicio de expedición de certificados de autenticación web, que pueden ser combinados entre sí para la prestación de servicios complejos e innovadores.

Se establece un régimen jurídico específico para los citados servicios electrónicos de confianza cualificados, consecuente con las elevadas exigencias de supervisión y seguridad que soportan, y cuyo reflejo es la singular relevancia probatoria que poseen respecto de los servicios no cualificados. Se refuerza así la seguridad jurídica de las transacciones electrónicas entre empresas, particulares y Administraciones públicas.

III

La aplicabilidad directa del Reglamento no priva a los Estados miembros de toda capacidad normativa sobre la materia regulada, es más, aquellos están obligados a adaptar los ordenamientos nacionales para garantizar que aquella cualidad se haga efectiva. Esta adaptación puede exigir tanto la modificación o derogación de normas existentes, como la adopción de nuevas disposiciones llamadas a completar la regulación europea.

En tal sentido, el objetivo de la presente Ley, como se indicaba ut supra, es complementar el Reglamento (UE) 910/2014 en aquellos aspectos que este no ha armonizado y que se dejan al criterio de los Estados miembros. Por tanto, la Ley se abstiene de reproducir las previsiones del Reglamento, abordando únicamente aquellas cuestiones que la norma europea remite a la decisión de los Estados miembros o que no se encuentran armonizadas, adquiriendo la regulación coherencia y sentido en el marco de la normativa europea.

Así, en virtud del principio de proporcionalidad, esta Ley contiene la regulación imprescindible para cubrir aquellos aspectos previstos en el Reglamento (UE) 910/2014, como es el caso, entre otros, del régimen de previsión de riesgo de los prestadores cualificados, el régimen sancionador, la comprobación de la identidad y atributos de los solicitantes de un certificado cualificado, la inclusión de requisitos adicionales a nivel nacional para certificados cualificados tales como identificadores nacionales, o su tiempo máximo de vigencia, así como las condiciones para la suspensión de los certificados.

El Reglamento (UE) 910/2014 garantiza la equivalencia jurídica entre la firma electrónica cualificada y la firma manuscrita, pero permite a los Estados miembros determinar los

efectos de las otras firmas electrónicas y de los servicios electrónicos de confianza en general. En este aspecto, se modifica la regulación anterior al atribuir a los documentos electrónicos para cuya producción o comunicación se haya utilizado un servicio de confianza cualificado una ventaja probatoria. A este respecto, se simplifica la prueba, pues basta la mera constatación de la inclusión del citado servicio en la lista de confianza de prestadores cualificados de servicios electrónicos regulada en el artículo 22 del Reglamento (UE) 910/2014.

Por lo que respecta a los certificados electrónicos, se introducen en la Ley varias disposiciones relativas a la expedición y contenido de los certificados cualificados, cuyo tiempo máximo de vigencia se mantiene en cinco años. En este sentido, no se permite a los prestadores de servicios el denominado «encadenamiento» en la renovación de certificados cualificados utilizando uno vigente, más que una sola vez, por razones de seguridad en el tráfico jurídico. Sin perjuicio de lo anterior, el Reglamento (UE) 910/2014 contempla la posibilidad de verificación de la identidad del solicitante de un certificado cualificado utilizando otros métodos de identificación reconocidos a escala nacional que garanticen una seguridad equivalente en términos de fiabilidad a la presencia física. Haciéndose eco de esta previsión, la Ley habilita a que reglamentariamente se regulen las condiciones y requisitos técnicos que lo harían posible.

Los certificados cualificados expedidos a personas físicas incluirán el número de Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, salvo en los casos en los que el titular carezca de todos ellos. La misma regla se aplica en cuanto al número de identificación fiscal de las personas jurídicas o sin personalidad jurídica titulares de certificados cualificados, que en defecto de este han de utilizar un código que les identifique de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales.

En lo que se refiere a las obligaciones de los prestadores, la Ley establece el requisito de constitución de una garantía económica para la prestación de servicios cualificados de confianza. Se fija una cuantía mínima única de 1.500.000 euros, que se incrementa en 500.000 euros por cada tipo de servicio adicional que se preste, lo que se estima suficiente para cubrir los riesgos derivados del servicio, tiene en cuenta la diversidad de servicios en el mercado y no penaliza a los prestadores con mayor oferta.

Una de las exigencias del Reglamento (UE) 910/2014 se centra en garantizar la seguridad de los servicios de confianza frente a actos deliberados o fortuitos que afecten a sus productos, redes o sistemas de información. En este sentido, todos los prestadores de servicios de confianza, cualificados y no cualificados, están sometidos a la obligación de adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan, así como de notificar al órgano de supervisión cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado. Esta Ley sanciona el incumplimiento de las citadas obligaciones.

En respuesta a la evolución de la tecnología y las demandas del mercado, el Reglamento (UE) 910/2014 abre la posibilidad de prestación de servicios innovadores basados en soluciones móviles y en la nube, como la firma y sello electrónicos remotos, en los que el entorno es gestionado por un prestador de servicios de confianza en nombre del titular. A fin de garantizar que estos servicios electrónicos obtengan el mismo reconocimiento jurídico que aquellos utilizados en un entorno completamente gestionado por el usuario, estos prestadores deben aplicar procedimientos de seguridad específicos y utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, para garantizar que el entorno es fiable y se utiliza bajo el control exclusivo del titular. Se pretende alcanzar, así, un equilibrio entre la facilidad para el acceso y el uso de los servicios, sin detrimento de la seguridad.

IV

Esta Ley deroga la Ley 59/2003, de 19 de diciembre, de firma electrónica, y con ella aquellos preceptos incompatibles con el Reglamento (UE) 910/2014.

Así sucede con los antiguos certificados de firma de personas jurídicas, introducidos por la citada Ley de firma electrónica. El nuevo paradigma instaurado por el mencionado

reglamento implica que únicamente las personas físicas están capacitadas para firmar electrónicamente, por lo que no prevé la emisión de certificados de firma electrónica a favor de personas jurídicas o entidades sin personalidad jurídica. A estas se reservan los sellos electrónicos, que permiten garantizar la autenticidad e integridad de documentos tales como facturas electrónicas. Sin perjuicio de lo anterior, las personas jurídicas podrán actuar por medio de los certificados de firma de aquellas personas físicas que legalmente les representen.

La Ley permite la posibilidad de que el órgano supervisor mantenga un servicio de difusión de información sobre los prestadores cualificados que operan en el mercado, con el fin de proporcionar a los usuarios información útil sobre los servicios que ofrecen en el desarrollo de su actividad.

Mediante la presente Ley se deroga también el artículo 25 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, referido a los terceros de confianza, debido a que los servicios ofrecidos por este tipo de proveedores se encuentran subsumidos en los tipos regulados por el Reglamento (UE) 910/2014, fundamentalmente en los servicios de entrega electrónica certificada y de conservación de firmas y sellos electrónicos.

V

Si bien la prestación de servicios electrónicos de confianza se realiza en régimen de libre competencia, el Reglamento (UE) 910/2014 prevé, para los servicios cualificados, un sistema de verificación previa de cumplimiento de los requisitos que en él se imponen. Así, se diseña un sistema mixto de colaboración público-privada para la supervisión de los prestadores cualificados, pues su inclusión en la lista de confianza, que permite iniciar esa actividad, debe basarse en un informe de evaluación de la conformidad emitido por un organismo de evaluación acreditado por un organismo nacional de acreditación, establecido en alguno de los Estados miembros de la Unión Europea. A partir de entonces, los prestadores cualificados deberán remitir el citado informe al menos cada veinticuatro meses.

Por su parte, los prestadores de servicios no cualificados pueden prestar servicios sin verificación previa de cumplimiento de requisitos, sin perjuicio de su sujeción a las potestades de seguimiento y control posterior de la Administración. No obstante, deberán comunicar al órgano supervisor la prestación del servicio en el plazo de tres meses desde que inicien su actividad, a los meros efectos de conocer su existencia y posibilitar su supervisión.

Por último, se define el régimen sancionador aplicable a los prestadores cualificados y no cualificados de servicios electrónicos de confianza, sin perjuicio de la posibilidad ya prevista en el artículo 20.3 del Reglamento (UE) 910/2014 de retirar la cualificación al prestador o servicio que presta, y su exclusión de la lista de confianza, en determinados supuestos. Asimismo, se han adecuado las cuantías de las sanciones, reduciéndose a la mitad la máxima imponible respecto a la legislación anterior, y se ha previsto la división en tramos de la horquilla sancionadora para la determinación de la multa imponible, en atención a los criterios de graduación concurrentes.

VI

Con arreglo a todo lo anterior, la presente Ley contiene veinte artículos, cuatro disposiciones adicionales, dos transitorias, una disposición derogatoria y siete disposiciones finales.

Las disposiciones adicionales se refieren: la primera a Fe pública y servicios electrónicos de confianza; la segunda a los efectos jurídicos de los sistemas utilizados en las Administraciones públicas; la tercera al Documento Nacional de Identidad y sus certificados electrónicos, y la cuarta al secreto de la identidad de los miembros del Centro Nacional de Inteligencia.

La disposición transitoria primera se refiere a la comunicación de actividad por prestadores de servicios no cualificados ya existentes, y la disposición transitoria segunda mantiene en vigor el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica, el

cual constituye desarrollo reglamentario parcial de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

En las disposiciones finales se modifican diversas leyes. En la primera, la Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información, de forma que las empresas que presten servicios al público en general de especial trascendencia económica deberán disponer de un medio seguro de interlocución telemática, no necesariamente basado en certificados electrónicos. Con ello, se flexibiliza la norma y se da cabida a otros medios de identificación generalmente usados en el sector privado.

En la disposición final segunda, se modifica la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, con objeto de adaptarla al nuevo marco regulatorio de los servicios electrónicos de confianza definido en esta Ley y en el Reglamento (UE) 910/2014.

En la disposición final tercera, se modifica la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, para adaptar su regulación al Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, referente a plataformas digitales.

En la disposición final cuarta se introduce una nueva disposición adicional séptima en la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio, para adaptar su regulación al Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimientos de los clientes en el mercado interior.

La disposición final quinta contiene el título competencial, en virtud del cual la Ley se dicta al amparo de las competencias exclusivas que corresponden al Estado en materia de legislación civil, telecomunicaciones y seguridad pública, conforme al artículo 149.1.8.ª, 21.ª y 29.ª de la Constitución Española. El artículo 3 y la disposición final segunda se dictan, además, al amparo de lo previsto en el artículo 149.1.6.ª de la Constitución, el cual atribuye al Estado competencia exclusiva en materia de legislación procesal. Por su parte la disposición adicional segunda se dicta al amparo de lo previsto en el artículo 149.1.18.ª de la Constitución, en relación con la competencia estatal exclusiva sobre las bases del régimen jurídico de las Administraciones públicas y el procedimiento administrativo común.

Finalmente las disposiciones finales sexta y séptima se refieren al desarrollo reglamentario de la Ley y a su entrada en vigor, respectivamente.

## TÍTULO I

## Disposiciones generales

**Artículo 1.** *Objeto de la Ley.*

La presente Ley tiene por objeto regular determinados aspectos de los servicios electrónicos de confianza, como complemento del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

**Artículo 2.** *Ámbito de aplicación.*

Esta Ley se aplicará a los prestadores públicos y privados de servicios electrónicos de confianza establecidos en España.

Así mismo, se aplicará a los prestadores residentes o domiciliados en otro Estado que tengan un establecimiento permanente situado en España, siempre que ofrezcan servicios no supervisados por la autoridad competente de otro país de la Unión Europea.

**Artículo 3.** *Efectos jurídicos de los documentos electrónicos.*

1. Los documentos electrónicos públicos, administrativos y privados, tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

2. La prueba de los documentos electrónicos privados en los que se hubiese utilizado un servicio de confianza no cualificado se regirá por lo dispuesto en el apartado 3 del artículo 326 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Si el servicio fuese cualificado, se estará a lo previsto en el apartado 4 del mismo precepto.

## TÍTULO II

## Certificados electrónicos

**Artículo 4.** *Vigencia y caducidad de los certificados electrónicos.*

1. Los certificados electrónicos se extinguen por caducidad a la expiración de su período de vigencia, o mediante revocación por los prestadores de servicios electrónicos de confianza en los supuestos previstos en el artículo siguiente.

2. El período de vigencia de los certificados cualificados no será superior a cinco años.

Dicho período se fijará en atención a las características y tecnología empleada para generar los datos de creación de firma, sello, o autenticación de sitio web.

**Artículo 5.** *Revocación y suspensión de los certificados electrónicos.*

1. Los prestadores de servicios electrónicos de confianza extinguirán la vigencia de los certificados electrónicos mediante revocación en los siguientes supuestos:

a) Solicitud formulada por el firmante, la persona física o jurídica representada por este, un tercero autorizado, el creador del sello o el titular del certificado de autenticación de sitio web.

b) Violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del prestador de servicios de confianza, o de autenticación de sitio web, o utilización indebida de dichos datos por un tercero.

c) Resolución judicial o administrativa que lo ordene.

d) Fallecimiento del firmante; capacidad modificada judicialmente sobrevenida, total o parcial, del firmante; extinción de la personalidad jurídica o disolución del creador del sello en el caso de tratarse de una entidad sin personalidad jurídica, y cambio o pérdida de control sobre el nombre de dominio en el supuesto de un certificado de autenticación de sitio web.

e) Terminación de la representación en los certificados electrónicos con atributo de representante. En este caso, tanto el representante como la persona o entidad representada están obligados a solicitar la revocación de la vigencia del certificado en cuanto se produzca la modificación o extinción de la citada relación de representación.

f) Cese en la actividad del prestador de servicios de confianza salvo que la gestión de los certificados electrónicos expedidos por aquel sea transferida a otro prestador de servicios de confianza.

g) Descubrimiento de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo.

h) En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de los certificados no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.

i) Cualquier otra causa lícita prevista en la declaración de prácticas del servicio de confianza.

2. Los prestadores de servicios de confianza suspenderán la vigencia de los certificados electrónicos en los supuestos previstos en las letras a), c) y h) del apartado anterior, así como en los casos de duda sobre la concurrencia de las circunstancias previstas en sus letras b) y g), siempre que sus declaraciones de prácticas de certificación prevean la posibilidad de suspender los certificados.

3. En su caso, y de manera previa o simultánea a la indicación de la revocación o suspensión de un certificado electrónico en el servicio de consulta sobre el estado de validez o revocación de los certificados por él expedidos, el prestador de servicios electrónicos de confianza comunicará al titular, por un medio que acredite la entrega y recepción efectiva

siempre que sea factible, esta circunstancia, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

En los casos de suspensión, la vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el prestador no la hubiera levantado.

**Artículo 6.** *Identidad y atributos de los titulares de certificados cualificados.*

1. La identidad del titular en los certificados cualificados se consignará de la siguiente forma:

a) En el supuesto de certificados de firma electrónica y de autenticación de sitio web expedidos a personas físicas, por su nombre y apellidos y su número de Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, o a través de un pseudónimo que conste como tal de manera inequívoca. Los números anteriores podrán sustituirse por otro código o número identificativo únicamente en caso de que el titular carezca de todos ellos por causa lícita, siempre que le identifique de forma unívoca y permanente en el tiempo.

b) En el supuesto de certificados de sello electrónico y de autenticación de sitio web expedidos a personas jurídicas, por su denominación o razón social y su número de identificación fiscal. En defecto de este, deberá indicarse otro código identificativo que le identifique de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales.

2. Si los certificados admiten una relación de representación incluirán la identidad de la persona física o jurídica representada en las formas previstas en el apartado anterior, así como una indicación del documento, público si resulta exigible, que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

**Artículo 7.** *Comprobación de la identidad y otras circunstancias de los solicitantes de un certificado cualificado.*

1. La identificación de la persona física que solicite un certificado cualificado exigirá su personación ante los encargados de verificarla y se acreditará mediante el Documento Nacional de Identidad, pasaporte u otros medios admitidos en Derecho. Podrá prescindirse de la personación de la persona física que solicite un certificado cualificado si su firma en la solicitud de expedición de un certificado cualificado ha sido legitimada en presencia notarial.

2. Reglamentariamente, mediante Orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, se determinarán otras condiciones y requisitos técnicos de verificación de la identidad a distancia y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física según su evaluación por un organismo de evaluación de la conformidad. La determinación de dichas condiciones y requisitos técnicos se realizará a partir de los estándares que, en su caso, hayan sido determinados a nivel comunitario.

Serán considerados métodos de identificación reconocidos a escala nacional, a los efectos de lo previsto en el presente apartado, aquellos que aporten una seguridad equivalente en términos de fiabilidad a la presencia física y cuya equivalencia en el nivel de seguridad sea certificada por un organismo de evaluación de la conformidad, de acuerdo con lo previsto en la normativa en materia de servicios electrónicos de confianza.

3. La forma en que se ha procedido a identificar a la persona física solicitante podrá constar en el certificado. En otro caso, los prestadores de servicios de confianza deberán colaborar entre sí para determinar cuándo se produjo la última personación.

4. En el caso de certificados cualificados de sello electrónico y de firma electrónica con atributo de representante, los prestadores de servicios de confianza comprobarán, además de los datos señalados en los apartados anteriores, los datos relativos a la constitución y personalidad jurídica, y a la persona o entidad representada, respectivamente, así como la extensión y vigencia de las facultades de representación del solicitante mediante los documentos, públicos si resultan exigibles, que sirvan para acreditar los extremos citados de

manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. Esta comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

5. Cuando el certificado cualificado contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, estas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.

6. Lo dispuesto en los apartados anteriores podrá no ser exigible cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de confianza en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubiese empleado el medio señalado en el apartado 1 y el período de tiempo transcurrido desde la identificación fuese menor de cinco años.

7. El Ministerio de Asuntos Económicos y Transformación Digital velará por que los prestadores cualificados de servicios electrónicos de confianza puedan contribuir a la elaboración de la norma reglamentaria prevista en el apartado 2 del presente artículo, de acuerdo con lo previsto en el artículo 26.6 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

## TÍTULO III

## Obligaciones y responsabilidad de los prestadores de servicios electrónicos de confianza

**Artículo 8.** *Protección de los datos personales.*

1. El tratamiento de los datos personales que precisen los prestadores de servicios electrónicos de confianza para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta Ley se sujetará a lo dispuesto en la legislación aplicable en materia de protección de datos de carácter personal.

2. Los prestadores de servicios electrónicos de confianza que consignen un pseudónimo en un certificado electrónico deberán constatar la verdadera identidad del titular del certificado y conservar la documentación que la acredite.

3. Dichos prestadores de servicios de confianza estarán obligados a revelar la citada identidad cuando lo soliciten los órganos judiciales y otras autoridades públicas en el ejercicio de funciones legalmente atribuidas, con sujeción a lo dispuesto en la legislación aplicable en materia de protección de datos personales.

**Artículo 9.** *Obligaciones de los prestadores de servicios electrónicos de confianza.*

1. Los prestadores de servicios electrónicos de confianza deberán:

a) Publicar información veraz y acorde con esta Ley y el Reglamento (UE) 910/2014.

b) No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.

En este caso, utilizarán sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, y se aplicarán procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado. Además, deberán custodiar y proteger los datos de creación de firma, sello o autenticación de sitio web frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

2. Los prestadores de servicios de confianza que expidan certificados electrónicos deberán disponer de un servicio de consulta sobre el estado de validez o revocación de los certificados emitidos accesible al público.

3. Los prestadores cualificados de servicios electrónicos de confianza deberán cumplir las siguientes obligaciones adicionales:

a) El período de tiempo durante el que deberán conservar la información relativa a los servicios prestados de acuerdo con el artículo 24.2.h) del Reglamento (UE) 910/2014, será de 15 años desde la extinción del certificado o la finalización del servicio prestado.

En caso de que expidan certificados cualificados de sello electrónico o autenticación de sitio web a personas jurídicas, los prestadores de servicios de confianza registrarán también la información que permita determinar la identidad de la persona física a la que se hayan entregado los citados certificados, para su identificación en procedimientos judiciales o administrativos.

b) Constituir un seguro de responsabilidad civil por importe mínimo de 1.500.000 euros, excepto si el prestador pertenece al sector público. Si presta más de un servicio cualificado de los previstos en el Reglamento (UE) 910/2014, se añadirán 500.000 euros más por cada tipo de servicio.

La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea coherente con lo dispuesto en el párrafo anterior.

Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto.

c) El prestador cualificado que vaya a cesar en su actividad deberá comunicarlo a los clientes a los que preste sus servicios y al órgano de supervisión con una antelación mínima de dos meses al cese efectivo de la actividad, por un medio que acredite la entrega y recepción efectiva siempre que sea factible. El plan de cese del prestador de servicios puede incluir la transferencia de clientes, una vez acreditada la ausencia de oposición de los mismos, a otro prestador cualificado, el cual podrá conservar la información relativa a los servicios prestados hasta entonces.

Igualmente, comunicará al órgano de supervisión cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.

d) Enviar el informe de evaluación de la conformidad al Ministerio de Asuntos Económicos y Transformación Digital en los términos previstos en el artículo 20.1 del Reglamento (UE) 910/2014. El incumplimiento de esta obligación conllevará la retirada de la cualificación al prestador y al servicio que este presta, y su eliminación de la lista de confianza prevista en el artículo 22 del citado Reglamento, previo requerimiento al prestador del servicio para que cese en el citado incumplimiento.

**Artículo 10.** *Responsabilidad de los prestadores de servicios electrónicos de confianza.*

Los prestadores de servicios electrónicos de confianza asumirán toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios electrónicos de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado.

**Artículo 11.** *Limitaciones de responsabilidad de los prestadores de servicios electrónicos de confianza.*

1. El prestador de servicios electrónicos de confianza no será responsable de los daños y perjuicios ocasionados a la persona a la que ha prestado sus servicios o a terceros de buena fe, si esta incurre en alguno de los supuestos previstos en el Reglamento (UE) 910/2014 o en los siguientes:

a) No haber proporcionado al prestador de servicios de confianza información veraz, completa y exacta para la prestación del servicio de confianza, en particular, sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada, actuando con la debida diligencia, por el prestador de servicios.

b) La falta de comunicación sin demora indebida al prestador de servicios de cualquier modificación de las circunstancias que incidan en la prestación del servicio de confianza, en particular, aquellas reflejadas en el certificado electrónico.

c) Negligencia en la conservación de sus datos de creación de firma, sello o autenticación de sitio web, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación de estos o, en su caso, de los medios que den acceso a ellos.

d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma, sello o autenticación de sitio web o, en su caso, de los medios que den acceso a ellos.

e) Utilizar los datos de creación de firma, sello o autenticación de sitio web cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de confianza le notifique la extinción o suspensión de su vigencia.

2. El prestador de servicios de confianza tampoco será responsable por los daños y perjuicios si el destinatario actúa de forma negligente. Se entenderá que el destinatario actúa de forma negligente cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico, o cuando no verifique la firma o sello electrónico.

3. El prestador de servicios de confianza no será responsable por los daños y perjuicios en caso de inexactitud de los datos que consten en el certificado electrónico si estos le han sido acreditados mediante documento público u oficial, inscrito en un registro público si así resulta exigible.

**Artículo 12.** *Inicio de la prestación de servicios electrónicos de confianza no cualificados.*

Los prestadores de servicios de confianza no cualificados no necesitan verificación administrativa previa de cumplimiento de requisitos para iniciar su actividad, pero deberán comunicar su actividad al Ministerio de Asuntos Económicos y Transformación Digital en el plazo de tres meses desde que la inicien, que publicará en su página web el listado de prestadores de servicios de confianza no cualificados en una lista diferente a la de los prestadores de servicios de confianza cualificados, con la descripción detallada y clara de las características propias y diferenciales de los prestadores cualificados y de los prestadores no cualificados.

En el mismo plazo deberán comunicar la modificación de los datos inicialmente transmitidos y el cese de su actividad.

**Artículo 13.** *Obligaciones de seguridad de la información.*

1. Los prestadores cualificados y no cualificados de servicios electrónicos de confianza notificarán al Ministerio de Asuntos Económicos y Transformación Digital las violaciones de seguridad o pérdidas de la integridad señaladas en el artículo 19.2 del Reglamento (UE) 910/2014, sin perjuicio de su notificación a la Agencia Española de Protección de Datos, a otros organismos relevantes o a las personas afectadas.

2. Los prestadores de servicios tienen la obligación de tomar las medidas necesarias para resolver los incidentes de seguridad que les afecten.

3. Los prestadores de servicios ampliarán, en un plazo máximo de un mes tras la notificación del incidente y, de haber tenido lugar, tras su resolución, la información suministrada en la notificación inicial con arreglo a las directrices y formularios que pueda establecer el Ministerio de Asuntos Económicos y Transformación Digital.

## TÍTULO IV

## Supervisión y control

**Artículo 14.** *Órgano de supervisión.*

1. El Ministerio de Asuntos Económicos y Transformación Digital, como órgano de supervisión, controlará el cumplimiento por los prestadores de servicios electrónicos de confianza cualificados y no cualificados que ofrezcan sus servicios al público de las obligaciones establecidas en el Reglamento (UE) 910/2014 y en esta Ley.

2. El Ministerio de Asuntos Económicos y Transformación Digital podrá acordar las medidas apropiadas para el cumplimiento del Reglamento (UE) 910/2014 y de esta Ley.

En particular, podrá dictar directrices para la elaboración y comunicación de informes y documentos, así como recomendaciones para el cumplimiento de las obligaciones técnicas y de seguridad exigibles a los servicios de confianza, así como sobre requisitos y normas técnicas de auditoría y certificación para la evaluación de la conformidad de los prestadores cualificados de servicios de confianza. Al efecto, se tendrán en consideración las normas, instrucciones, guías y recomendaciones emitidas por el Centro Criptológico Nacional en el marco de sus competencias, así como informes, especificaciones o normas elaboradas por la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) o por organismos de estandarización europeos e internacionales.

**Artículo 15.** *Actuaciones inspectoras.*

1. El Ministerio de Asuntos Económicos y Transformación Digital realizará las actuaciones inspectoras que sean precisas para el ejercicio de su función de supervisión y control. Los funcionarios adscritos al Ministerio de Asuntos Económicos y Transformación Digital que realicen la inspección tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

2. El Ministerio de Asuntos Económicos y Transformación Digital podrá recurrir a entidades independientes y técnicamente cualificadas para que le asistan en las labores de supervisión y control sobre los prestadores de servicios de confianza que le asigna el Reglamento (UE) 910/2014 y esta Ley.

3. Podrá requerirse la realización de pruebas en laboratorios o entidades especializadas para acreditar el cumplimiento de determinados requisitos. En este caso, los prestadores de servicios correrán con los gastos que ocasione esta evaluación.

**Artículo 16.** *Mantenimiento de la lista de confianza.*

1. El Ministerio de Asuntos Económicos y Transformación Digital establecerá, mantendrá y publicará la lista de confianza con información relativa a los prestadores cualificados de servicios de confianza sujetos a esta Ley, junto con la información relacionada con los servicios de confianza cualificados prestados por ellos, según lo previsto en el artículo 22 del Reglamento (UE) 910/2014.

2. El plazo máximo para dictar y notificar resolución en el procedimiento de verificación previa de cumplimiento de los requisitos establecidos en el citado Reglamento será de 6 meses, transcurridos los cuales se podrá entender desestimada la solicitud.

3. La revocación de la cualificación a un prestador o a un servicio mediante su retirada de la lista de confianza es independiente de la aplicación del régimen sancionador.

**Artículo 17.** *Información y colaboración.*

1. Los prestadores de servicios de confianza, la entidad nacional de acreditación, los organismos de evaluación de la conformidad, los organismos de certificación y cualquier otra persona o entidad relacionada con el prestador de servicios de confianza, tienen la obligación de facilitar al Ministerio de Asuntos Económicos y Transformación Digital toda la información y colaboración precisas para el ejercicio de sus funciones.

Si el organismo de certificación perteneciera a la Autoridad Nacional de Certificación de la Ciberseguridad o estuviese supervisado por ella, se acordarán con dicha Autoridad los mecanismos de colaboración y el contenido de la información necesaria.

Los prestadores de servicios de confianza deberán permitir a sus funcionarios o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.6 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquellas.

2. La información referente a los prestadores cualificados de servicios de confianza podrá ser objeto de publicación en la dirección de Internet del Ministerio de Asuntos Económicos y Transformación Digital para su difusión y conocimiento.

3. A más tardar el 1 de febrero de cada año, los prestadores cualificados de servicios de confianza remitirán al Ministerio de Asuntos Económicos y Transformación Digital un informe

sobre sus datos de actividad del año civil precedente, con objeto de cumplimiento por parte de este de las obligaciones de información a la Comisión Europea.

4. El Ministerio de Asuntos Económicos y Transformación Digital informará a la Agencia Española de Protección de Datos en caso de resultar infringidas las normas sobre protección de datos de carácter personal, así como sobre los incidentes en materia de seguridad que impliquen violaciones de los datos de carácter personal.

## TÍTULO V

## Infracciones y sanciones

**Artículo 18.** *Infracciones.*

1. Las infracciones de los preceptos del Reglamento (UE) 910/2014 y de esta Ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) La comisión de una infracción grave en el plazo de dos años desde que hubiese sido sancionado por una infracción grave de la misma naturaleza, contados desde que recaiga la resolución sancionadora firme.

b) La expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado o al poder de representación de quien lo solicita en su nombre, señaladas en el Reglamento (UE) 910/2014 y en esta Ley, cuando ello afecte a la mayoría de los certificados cualificados expedidos en el año anterior al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este periodo es menor.

3. Son infracciones graves:

a) La resistencia, obstrucción, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley.

b) Actuar en el mercado como prestador cualificado de servicios de confianza, ofrecer servicios de confianza como cualificados o utilizar la etiqueta de confianza «UE» sin haber obtenido la cualificación de los citados servicios.

c) En caso de que el prestador expida certificados electrónicos, almacenar o copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.

d) No proteger adecuadamente los datos de creación de firma, sello o autenticación de sitio web cuya gestión se le haya encomendado en la forma establecida en el artículo 9.1.b) de esta Ley.

e) No registrar o conservar la información a la que se refiere el artículo 9.3.a) de esta Ley.

f) El incumplimiento de la obligación de notificación de incidentes establecida en el artículo 19.2 del Reglamento (UE) 910/2014, en los términos previstos en el artículo 13 de esta Ley.

g) En caso de prestadores cualificados de servicios de confianza, el incumplimiento de alguna de las obligaciones establecidas en los artículos 24.2, letras b), c), d), e), f), g), h), y k), 24.3 y 24.4 del Reglamento (UE) 910/2014, con las precisiones establecidas, en su caso, por esta Ley.

h) La expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado o al poder de representación de quien lo solicita en su nombre, señaladas en el Reglamento (UE) 910/2014 y en esta Ley, cuando no constituya infracción muy grave.

i) La ausencia de adopción de medidas, o la adopción de medidas insuficientes, para la resolución de los incidentes de seguridad en los productos, redes y sistemas de información, en el plazo de diez días desde que aquellos se hubieren producido.

j) El incumplimiento de las resoluciones dictadas por el Ministerio de Asuntos Económicos y Transformación Digital para requerir a un prestador de servicios de confianza

que corrija cualquier incumplimiento de los requisitos establecidos en esta Ley y en el Reglamento (UE) 910/2014.

k) La falta o deficiente presentación de información solicitada por parte del Ministerio de Asuntos Económicos y Transformación Digital en su función de inspección y control, a partir del segundo requerimiento.

l) No cumplir con las obligaciones de constatar la verdadera identidad del titular de un certificado electrónico y de conservar la documentación que la acredite, en caso de consignación de un pseudónimo.

m) El incumplimiento por parte de los prestadores cualificados y no cualificados de servicios de confianza de la obligación establecida en el artículo 19.1 del Reglamento (UE) 910/2014 de adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que presten.

n) No extinguir la vigencia de los certificados electrónicos en los supuestos señalados en esta Ley.

o) La prestación de servicios cualificados careciendo del correspondiente seguro obligatorio, en los términos previstos en el artículo 9.3.b) de esta Ley.

4. Constituyen infracciones leves:

a) Publicar información no veraz o no acorde con esta Ley y el Reglamento (UE) 910/2014.

b) No comunicar el inicio de actividad, su modificación o cese por los prestadores de servicios no cualificados en el plazo establecido en el artículo 12 de esta Ley.

c) El incumplimiento por los prestadores cualificados de servicios de confianza de alguna de las obligaciones establecidas en el artículo 24.2, letras a) e i) del Reglamento (UE) 910/2014.

d) El incumplimiento por los prestadores cualificados de servicios de confianza de su obligación de remitir un informe anual de actividad al Ministerio de Asuntos Económicos y Transformación Digital antes del 1 de febrero de cada año.

e) El incumplimiento del deber de comunicación establecido en el artículo 9.3.c) de esta Ley.

f) La falta o deficiente presentación de información solicitada por parte del Ministerio de Asuntos Económicos y Transformación Digital en su función de inspección y control.

**Artículo 19.** *Sanciones.*

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán al infractor las siguientes sanciones:

a) Por la comisión de infracciones muy graves, una multa por importe de 150.001 hasta 300.000 euros.

b) Por la comisión de infracciones graves, una multa por importe de 50.001 hasta 150.000 euros.

c) Por la comisión de infracciones leves, una multa por importe de hasta 50.000 euros.

2. La cuantía de las sanciones que se impongan se determinará aplicando una graduación de importe mínimo, medio y máximo a cada nivel de infracción, teniendo en cuenta lo siguiente:

a) El grado de culpabilidad o la existencia de intencionalidad.

b) La continuidad o persistencia en la conducta infractora.

c) La naturaleza y cuantía de los perjuicios causados.

d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa.

e) El volumen de facturación del prestador responsable.

f) El número de personas afectadas por la infracción.

g) La gravedad del riesgo generado por la conducta.

h) Las acciones realizadas por el prestador encaminadas a paliar los efectos o consecuencias de la infracción.

3. Las resoluciones sancionadoras por la comisión de infracciones muy graves serán publicadas en el sitio de Internet del Ministerio de Asuntos Económicos y Transformación Digital, con indicación, en su caso, de los recursos interpuestos contra ellas.

**Artículo 19 bis.** *Apercibimiento.*

1. Los órganos con competencia sancionadora, atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el artículo anterior, podrán acordar no iniciar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable, a fin de que en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que, en cada caso, resulten pertinentes, siempre que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta ley.

2. Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

**Artículo 20.** *Potestad sancionadora.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

2. La potestad sancionadora regulada en esta ley se ejercerá de conformidad con lo establecido al respecto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en sus normas de desarrollo. El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de iniciación. El plazo máximo de duración del procedimiento simplificado será de tres meses.

**Disposición adicional primera.** *Fe pública y servicios electrónicos de confianza.*

Lo dispuesto en esta Ley no sustituye ni modifica las normas que regulan las funciones que corresponden a los funcionarios que tengan legalmente atribuida la facultad de dar fe en documentos en lo que se refiere al ámbito de sus competencias.

**Disposición adicional segunda.** *Efectos jurídicos de los sistemas utilizados en las Administraciones públicas.*

Todos los sistemas de identificación, firma y sello electrónico previstos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, tendrán plenos efectos jurídicos.

**Disposición adicional tercera.** *Documento Nacional de Identidad y sus certificados electrónicos.*

1. El Documento Nacional de Identidad electrónico es el Documento Nacional de Identidad que permite acreditar electrónicamente la identidad personal de su titular, en los términos establecidos en el artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, así como la firma electrónica de documentos.

2. Todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del Documento Nacional de Identidad para acreditar la identidad y los demás datos personales del titular que consten en el mismo, así como la identidad del firmante y la integridad de los documentos firmados con sus certificados electrónicos.

3. Los órganos competentes del Ministerio del Interior para la expedición del Documento Nacional de Identidad cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios electrónicos de confianza que expidan certificados cualificados.

4. Sin perjuicio de la aplicación de la normativa vigente en materia del Documento Nacional de Identidad en todo aquello que se adecúe a sus características particulares, el Documento Nacional de Identidad se regirá por su normativa específica.

**Disposición adicional cuarta.** *Secreto de la identidad de los miembros del Centro Nacional de Inteligencia.*

Lo dispuesto en los artículos 7 y 8 de esta Ley se entenderá sin perjuicio de lo dispuesto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, en relación con la obligación de guardar secreto sobre la identidad de sus miembros.

**Disposición transitoria primera.** *Comunicación de actividad por prestadores de servicios no cualificados ya existentes.*

Los prestadores de servicios no cualificados que ya vinieran prestando servicios deberán comunicar su actividad al Ministerio de Asuntos Económicos y Transformación Digital en el plazo de tres meses a contar desde la entrada en vigor de esta Ley.

Se exceptúan aquellos que hubieran comunicado los servicios prestados al Ministerio de Asuntos Económicos y Transformación Digital antes de la entrada en vigor de esta Ley.

**Disposición transitoria segunda.** *Desarrollo reglamentario del Documento Nacional de Identidad.*

Hasta que se desarrolle reglamentariamente el Documento Nacional de Identidad, se mantendrá en vigor el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

**Disposición derogatoria.**

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley, y en particular:

a) La Ley 59/2003, de 19 de diciembre, de firma electrónica.

b) El artículo 25 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

c) La Orden del Ministerio de Fomento de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

**Disposición final primera.** *Modificación de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.*

Se modifica el apartado 1 del artículo 2 de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, que queda redactado como sigue:

> «1. Sin perjuicio de la utilización de otros medios de comunicación a distancia con los clientes, las empresas que presten servicios al público en general de especial trascendencia económica deberán facilitar a sus usuarios un medio seguro de interlocución telemática que les permita la realización de, al menos, los siguientes trámites:
>
> a) Contratación electrónica de servicios, suministros y bienes, la modificación y finalización o rescisión de los correspondientes contratos, así como cualquier acto o negocio jurídico entre las partes, sin perjuicio de lo establecido en la normativa sectorial.
>
> b) Consulta de sus datos de cliente, que incluirán información sobre su historial de facturación de, al menos, los últimos tres años y el contrato suscrito, incluidas las condiciones generales si las hubiere.
>
> c) Presentación de quejas, incidencias, sugerencias y, en su caso, reclamaciones, garantizando la constancia de su presentación para el consumidor y asegurando una atención personal directa.
>
> d) Ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la normativa reguladora de protección de datos de carácter personal.»

**Disposición final segunda.** *Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.*

Uno. Se modifica el apartado 3 del artículo 326 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que queda redactado en los siguientes términos:

«3. Cuando la parte a quien interese la eficacia de un documento electrónico lo solicite o se impugne su autenticidad, integridad, precisión de fecha y hora u otras características del documento electrónico que un servicio electrónico de confianza no cualificado de los previstos en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, permita acreditar, se procederá con arreglo a lo establecido en el apartado 2 del presente artículo y en el Reglamento (UE) n.º 910/2014.»

Dos. Se añade un apartado 4 al citado artículo 326, con el siguiente tenor:

«4. Si se hubiera utilizado algún servicio de confianza cualificado de los previstos en el Reglamento citado en el apartado anterior, se presumirá que el documento reúne la característica cuestionada y que el servicio de confianza se ha prestado correctamente si figuraba, en el momento relevante a los efectos de la discrepancia, en la lista de confianza de prestadores y servicios cualificados.

Si aun así se impugnare el documento electrónico, la carga de realizar la comprobación corresponderá a quien haya presentado la impugnación. Si dichas comprobaciones obtienen un resultado negativo, serán las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 300 a 1200 euros.»

**Disposición final tercera.** *Modificación de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.*

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, se modifica en los siguientes términos:

Uno. Se añade un nuevo artículo 12 ter que queda redactado como sigue:

**«Artículo 12 ter.** *Obligaciones relativas a la portabilidad de datos no personales.*

Los proveedores de servicios de intermediación que alojen o almacenen datos de usuarios a los que presten servicios de redes sociales o servicios de la sociedad de la información equivalentes deberán remitir a dichos usuarios, a su solicitud, los contenidos que les hubieran facilitado, sin impedir su transmisión posterior a otro proveedor. La remisión deberá efectuarse en un formato estructurado, de uso común y lectura mecánica.

Asimismo, deberán transmitir dichos contenidos directamente a otro proveedor designado por el usuario, siempre que sea técnicamente posible, según prevé el artículo 95 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Para el cumplimiento de estas obligaciones será aplicable lo dispuesto en el artículo 12.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.»

Dos. El primer párrafo del apartado 1 del artículo 35 queda redactado como sigue:

«1. El Ministerio de Asuntos Económicos y Transformación Digital controlará el cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo, en lo que se refiere a los servicios propios de la sociedad de la información, así como en el Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de

2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea, por parte de aquellos proveedores incluidos en su ámbito de aplicación.»

Tres. Se añade un nuevo artículo 36 bis que queda redactado como sigue:

**«Artículo 36 bis.** *Deber de comunicación de las organizaciones y asociaciones representativas de usuarios profesionales o de los usuarios de sitios web corporativos.*

Las organizaciones y asociaciones que posean un interés legítimo de representación de usuarios profesionales o de los usuarios de sitios web corporativos, y que, cumpliendo con los requisitos del artículo 14.3 del Reglamento (UE) 2019/1150, hubieren solicitado al Ministerio de Asuntos Económicos y Transformación Digital su inclusión en la lista elaborada al efecto por la Comisión Europea, notificarán inmediatamente al citado Ministerio cualquier circunstancia que afecte a su entidad que derive en un incumplimiento sobrevenido de los mencionados requisitos.»

Cuatro. El primer párrafo del artículo 37 queda redactado como sigue:

«Los prestadores de servicios de la sociedad de la información a los que les sea de aplicación la presente Ley, así como los proveedores incluidos en el ámbito de aplicación del Reglamento (UE) 2019/1150, están sujetos al régimen sancionador establecido en este Título.»

Cinco. Se añaden doce nuevas letras de la j) a la u) al apartado 3 del artículo 38 con la siguiente redacción:

«j) La exigencia del pago de un canon por atender la obligación prevista en el artículo 12 ter, fuera de los supuestos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679.

k) El incumplimiento habitual de la obligación prevista en el artículo 12 ter.

l) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación establecida en el apartado 5 del artículo 3 del Reglamento (UE) 2019/1150 en materia de visibilidad de la identidad del usuario profesional.

m) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de cualquiera de las obligaciones en materia de restricción, suspensión y terminación del servicio establecidas en los apartados 1, 2 y 3 del artículo 4 del Reglamento (UE) 2019/1150.

n) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea o proveedores de motores de búsqueda en línea de cualquiera de las obligaciones en materia de clasificación establecidas en el artículo 5 del Reglamento (UE) 2019/1150 que les resulten aplicables.

o) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de incluir en sus condiciones generales la información exigida en el artículo 6 del Reglamento (UE) 2019/1150 sobre los bienes y servicios auxiliares ofrecidos.

p) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea o los proveedores de motores de búsqueda en línea de la obligación de incluir en sus condiciones generales la información exigida en los apartados 1 y 2, respectivamente, con las precisiones establecidas en el apartado 3, del artículo 7 del Reglamento (UE) 2019/1150, en materia de tratamiento diferenciado de bienes o servicios.

q) El incumplimiento por parte de los proveedores de servicios de intermediación de la obligación establecida en la letra a) del artículo 8 del Reglamento (UE) 2019/1150, así como el incumplimiento habitual de las obligaciones contenidas en las letras b) y c) del citado precepto.

r) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de informar sobre el acceso a datos por parte de los usuarios profesionales establecida en el artículo 9 del Reglamento (UE) 2019/1150.

s) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de justificar las restricciones a la oferta de condiciones diferentes por otros medios prevista en el artículo 10 del Reglamento (UE) 2019/1150.

t) El incumplimiento por parte de los proveedores de servicios de intermediación en línea que no sean pequeñas empresas, de la obligación de establecer un sistema interno y gratuito para tramitar las reclamaciones de los usuarios profesionales, en los términos previstos por el artículo 11 del Reglamento (UE) 2019/1150.

u) El incumplimiento por parte de los proveedores de servicios de intermediación en línea que no sean pequeñas empresas, de la obligación de designar al menos dos mediadores, o de cualquier otra de las obligaciones en materia de mediación establecidas en el artículo 12 del Reglamento (UE) 2019/1150.»

Seis. Se añaden diez nuevas letras de la j) a la s) al apartado 4 del artículo 38 con la siguiente redacción:

«j) La exigencia del pago de un canon por atender la obligación prevista en el artículo 12 ter, cuando así lo permita el artículo 12.5 del Reglamento (UE) 2016/679, si su cuantía excediese el importe de los costes afrontados.

k) El incumplimiento de la obligación prevista en el artículo 12 ter, cuando no constituya infracción grave.

l) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación establecida en el apartado 5 del artículo 3 del Reglamento (UE) 2019/1150 en materia de visibilidad de la identidad del usuario profesional, cuando no constituya infracción grave.

m) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de cualquiera de las obligaciones en materia de restricción, suspensión y terminación del servicio establecidas en los apartados 1, 2 y 3 del artículo 4 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

n) El incumplimiento por parte de los proveedores de servicios de intermediación en línea o proveedores de motores de búsqueda en línea de cualquiera de las obligaciones en materia de clasificación establecidas en el artículo 5 del Reglamento (UE) 2019/1150 que les resulten aplicables, cuando no constituya infracción grave.

o) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de incluir en sus condiciones generales la información exigida en el artículo 6 del Reglamento (UE) 2019/1150 sobre los bienes y servicios auxiliares ofrecidos, cuando no constituya infracción grave.

p) El incumplimiento por parte de los proveedores de servicios de intermediación en línea y los proveedores de motores de búsqueda en línea de la obligación de incluir en sus condiciones generales la información exigida en los apartados 1 y 2, respectivamente, con las precisiones establecidas en el apartado 3, del artículo 7 del Reglamento (UE) 2019/1150, en materia de tratamiento diferenciado de bienes o servicios, cuando no constituya infracción grave.

q) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de las obligaciones en materia de cláusulas contractuales específicas establecidas en el artículo 8 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

r) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de informar sobre el acceso a datos por parte de los usuarios profesionales establecida en el artículo 9 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

s) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de justificar las restricciones a la oferta de condiciones diferentes por otros medios prevista en el artículo 10 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.»

Siete. El artículo 43 queda redactado como sigue:

**«Artículo 43.** *Competencia sancionadora.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren las letras a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en sus normas de desarrollo. El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de iniciación. El plazo máximo de duración del procedimiento simplificado será de tres meses.»

**Disposición final cuarta.** *Modificación de la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio.*

Se introduce una nueva disposición adicional séptima con el siguiente contenido:

**«Disposición adicional séptima.** *Incumplimiento de la prohibición de discriminación.*

El incumplimiento de la prohibición de discriminación prevista en el artículo 16.3 de esta Ley y el Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, de 28 de febrero de 2018, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE, se reputará desleal a los efectos de la Ley 3/1991, de 10 de enero, de Competencia Desleal, sin perjuicio del régimen de infracciones y sanciones contenido en el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.»

**Disposición final quinta.** *Título competencial.*

Esta Ley se dicta al amparo de las competencias exclusivas que corresponden al Estado en materia de legislación civil, telecomunicaciones y seguridad pública, conforme a lo dispuesto en el artículo 149.1.8.ª, 21.ª y 29.ª de la Constitución Española.

El artículo 3 y la disposición final segunda se dictan, además, al amparo de lo previsto en el artículo 149.1.6.ª de la Constitución, el cual atribuye al Estado competencia exclusiva en materia de legislación procesal. Por su parte la disposición adicional segunda se dicta al amparo de lo previsto en el artículo 149.1.18.ª de la Constitución, en relación con la competencia estatal exclusiva sobre las bases del régimen jurídico de las Administraciones públicas y el procedimiento administrativo común.

**Disposición final sexta.** *Desarrollo reglamentario.*

Se habilita al Gobierno para dictar las disposiciones reglamentarias que sean precisas para el desarrollo y aplicación de esta Ley.

**Disposición final séptima.** *Entrada en vigor.*

La presente Ley entrará en vigor al día siguiente al de su publicación en el «Boletín Oficial del Estado».

# § 47

## Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 299, de 13 de diciembre de 2012
Última modificación: sin modificaciones
Referencia: BOE-A-2012-15066

El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, establece, en su artículo 24, apartado 3, que la política de firma electrónica y de certificados en el ámbito de la Administración General del Estado y de sus organismos públicos será aprobada por el Consejo Superior de Administración Electrónica.

Así mismo, señala que el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados extractado se publicará en el «Boletín Oficial del Estado», mediante resolución del Secretario de Estado para la Función Pública, y de forma íntegra en la sede del punto de acceso general de la Administración General del Estado.

De conformidad con el Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas, las funciones de la Secretaría de Estado para la Función Pública son asumidas por la Secretaría de Estado de Administraciones Públicas.

El Consejo Superior de Administración Electrónica, en reunión de la Comisión Permanente de 30 de mayo de 2012, aprobó la Política de Firma Electrónica y de Certificados en el ámbito de la Administración General del Estado y de sus organismos públicos, de conformidad con lo previsto en el artículo 24, apartado 3, del citado Real Decreto 1671/2009.

En su virtud, y en aplicación de lo dispuesto en el mencionado artículo 24, apartado 3, del Real Decreto 1671/2009, esta Secretaría de Estado resuelve:

**Primero.**

Ordenar la publicación en el «Boletín Oficial del Estado» del Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados en el ámbito de la Administración General del Estado y de sus organismos públicos, adoptado por el Consejo Superior de Administración Electrónica, en reunión de la Comisión Permanente de 30 de mayo de 2012, en cumplimiento de lo previsto en el artículo 24, apartado 3, de Real Decreto 1671/2009, y que se incluye en esta Resolución como anexo.

**Segundo.**

Ordenar la publicación íntegra en la sede del punto de acceso general de la Administración General del Estado (ver datos de acceso en el siguiente apartado) de los documentos comprensivos de la política de firma electrónica basada en certificados en el ámbito de la Administración General del Estado y de sus organismos públicos y de los perfiles de los certificados electrónicos, constituidos por los anexos I, Política de firma electrónica y de certificados de la Administración General del Estado, y II, Perfiles de certificados electrónicos, en forma de documentos electrónicos en formato PDF firmados electrónicamente el día 19 de noviembre de 2012 por la Presidenta de la Comisión Permanente del Consejo Superior de Administración Electrónica, doña María Ester Arizmendi Gutiérrez, de forma que sus códigos de verificación electrónicos se puedan comprobar en la sede de la Secretaría de Estado de Administraciones Públicas en la dirección provisional https://sede.mpt.gob.es/valida, todo ello sin perjuicio de que puedan ser publicados en otras sedes electrónicas.

**Tercero.**

Ordenar la publicación extractada en el «Boletín Oficial del Estado» de los datos de acceso y códigos de verificación electrónicos de los documentos comprensivos de la política de firma electrónica basada en certificados en el ámbito de la Administración General del Estado y de sus organismos públicos y de los perfiles de los certificados electrónicos, constituidos por los anexos I, Política de firma electrónica y de certificados de la Administración General del Estado, y II, Perfiles de certificados electrónicos, para que se pueda verificar la integridad de los mismos (se incluyen códigos QR para acceder, desde dispositivos móviles, a los ficheros y a la información de los códigos de verificación respectivos):

Documento: Anexo I, Política de firma electrónica y de certificados de la Administración General del Estado.
Dirección o URL: https://sede.060.gob.es/politica_de_firma_anexo_1.pdf.
Tamaño de fichero: 178.383 bytes.
Código de verificación electrónico: C4075E8D7946EF14B65819F01C2D5F63.

Dirección o URL: CVE:

Documento: Anexo II, Perfiles de certificados electrónicos.
Dirección o URL: https://sede.060.gob.es/perfiles_de_certificados_anexo_2.pdf.
Tamaño de fichero: 363.674 bytes.
Código de verificación electrónico: 483AFA7835C0CF999551DF4992EE945D.

Dirección o URL: CVE:

**Cuarto.**

La política de firma electrónica y de certificados de la Administración General del Estado, se aplicará en el plazo de un mes siguiente a la publicación de esta Resolución en el «Boletín Oficial del Estado».

**ANEXO**

**Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados en el ámbito de la Administración General del Estado y de sus organismos públicos**

Doña Manuela de Paz Prieto, Secretaria de la Comisión Permanente del Consejo Superior de Administración Electrónica,

CERTIFICA, que en la 82.ª reunión de la Comisión Permanente del Consejo Superior de Administración Electrónica, celebrada en Madrid, en la sede del Ministerio de Hacienda y Administraciones Públicas, calle María de Molina, 50, el día treinta de mayo de dos mil doce, en cumplimiento del acuerdo sobre delegación de competencias en la Comisión Permanente, del Pleno del Consejo Superior de Administración Electrónica celebrado el 3 de abril de 2006, se adoptó, entre otros, el siguiente acuerdo:

Informar favorablemente la Resolución de la Secretaría de Estado de Administraciones Públicas, por la que se establece la Política de Firma Electrónica y de Certificados de la Administración General del Estado, en los términos que se recogen en los documentos que se acompañan como anexos, en ejercicio de las funciones atribuidas en el artículo 4.1.c) del Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados responsables de la Administración electrónica.

Se hace constar, en aplicación de lo dispuesto en el apartado 5 del artículo 27 de la Ley 30/1992, de 26 de noviembre, que el Acta de la sesión donde se adoptó el presente acuerdo se someterá a la aprobación de la Comisión Permanente en su siguiente reunión.

Y para que conste, se firma el presente certificado en Madrid, a 29 de junio de 2012.

# § 48

# Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica

Ministerio del Interior
«BOE» núm. 307, de 24 de diciembre de 2005
Última modificación: 30 de mayo de 2015
Referencia: BOE-A-2005-21163

La Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, en su artículo 9, reconoce el derecho de todos los españoles a que se les expida el Documento Nacional de Identidad, al que se atribuye el valor suficiente para acreditar, por sí solo, la identidad de las personas y le otorga la protección que a los documentos públicos y oficiales es reconocida por el ordenamiento jurídico.

La misma norma dispone la obligatoriedad del Documento Nacional de Identidad para los mayores de catorce años, salvo en los supuestos en que, conforme a lo previsto en la Ley, haya de ser sustituido por otro documento, y establece también que en el mismo figurarán la fotografía y la firma del titular, así como los datos personales que se determinen reglamentariamente.

En cuanto a la competencia para su expedición y gestión, la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, atribuye al Cuerpo Nacional de Policía, la de la expedición del Documento Nacional de Identidad, al recogerla expresamente entre las funciones que encomienda a este Instituto Policial, el cual la misma Ley dispone que dependerá del Ministerio del Interior.

Por otra parte, la Ley 59/2003, de 19 de diciembre, de firma electrónica, ha venido a atribuir al Documento Nacional de Identidad nuevos efectos y utilidades, como son los de poder acreditar electrónicamente la identidad y demás datos personales del titular que en él consten, así como la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica, cuya incorporación al mismo se establece.

La misma Ley, en el apartado primero de la disposición final segunda dispone que el Gobierno adaptará la regulación reglamentaría del Documento Nacional de Identidad a las previsiones de la referida Ley.

Asimismo, ha de señalarse que la normativa reglamentaria que regula los distintos aspectos del Documento Nacional de Identidad se encuentra dispersa en distintas disposiciones y data, en parte, de fechas anteriores a la vigencia de la Constitución, lo que genera disfunciones a la hora de su aplicación, derivadas tanto de la propia antigüedad de las normas, como de la dispersión de estas.

En este contexto, y a la vista del mandato legal contenido en la Ley 59/2003, antes citada, resulta imprescindible acometer la adecuación y ordenación de la normativa que regula el referido Documento, abordando aquellos aspectos derivados de las nuevas utilidades que se le atribuyen.

En su virtud, a propuesta del Ministro del Interior, con la aprobación previa del Ministro de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros, en su reunión del día 23 de diciembre de 2005,

D I S P O N G O :

**Artículo 1.** *Naturaleza y funciones.*

1. El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y conservación del mismo.

2. Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo.

3. A cada Documento Nacional de Identidad, se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter general.

4. Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

En el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento nacional de identidad contendrá, únicamente, la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado.

5. La firma electrónica realizada a través del Documento Nacional de Identidad tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

6. Ningún español podrá ser privado del Documento Nacional de Identidad, ni siquiera temporalmente, salvo en los casos y forma establecidos por las Leyes en los que haya de ser sustituido por otro documento.

**Artículo 2.** *Derecho y obligación de obtenerlo.*

1. Todos los españoles tendrán derecho a que se les expida el Documento Nacional de Identidad, siendo obligatoria su obtención por los mayores de catorce años residentes en España y para los de igual edad que, residiendo en el extranjero, se trasladen a España por tiempo no inferior a seis meses.

2. Todas las personas obligadas a obtener el Documento Nacional de Identidad lo están también a exhibirlo cuando fueren requeridas para ello por la Autoridad o sus Agentes.

**Artículo 3.** *Órgano competente para la expedición y gestión.*

1. Será competencia del Ministerio del Interior el ejercicio de las funciones relativas a la gestión, dirección, organización, desarrollo y administración de todos aquellos aspectos referentes a la expedición y confección del Documento Nacional de Identidad, conforme a lo previsto en la legislación en materia de seguridad ciudadana y de firma electrónica.

2. El ejercicio de las competencias a que se refiere el apartado anterior, incluida la emisión de los certificados de firma electrónica reconocidos, será realizado por la Dirección General de la Policía, a quien corresponderá también la custodia y responsabilidad de los archivos y ficheros, automatizados o no, relacionados con el Documento Nacional de Identidad. A tal efecto, la Dirección General de la Policía quedará sometida a las obligaciones impuestas al responsable del fichero por la Ley Orgánica 15/1999, de 13 de septiembre, de Protección de Datos de Carácter Personal.

**Artículo 4.** *Procedimiento de expedición.*

1. El Documento Nacional de Identidad se expedirá a solicitud del interesado en la forma y lugares que al efecto se determinen, para lo cual deberá aportar los documentos que se establecen en el artículo 5.1 de este Real Decreto.

2. En orden a facilitar a los ciudadanos la obtención del Documento Nacional de Identidad, el Ministerio del Interior en colaboración con el Ministerio de Administraciones Públicas adoptará las medidas oportunas para el fomento de la cooperación de los distintos órganos de las Administraciones Públicas con la Dirección General de la Policía.

**Artículo 5.** *Requisitos para la expedición.*

1. Para solicitar la expedición del Documento Nacional de Identidad será imprescindible la presencia física de la persona a quien se haya de expedir, el abono de la tasa legalmente establecida en cada momento y la presentación de los siguientes documentos:

a) Certificación literal de nacimiento expedida por el Registro Civil correspondiente. A estos efectos únicamente serán admitidas las certificaciones expedidas con una antelación máxima de seis meses a la fecha de presentación de la solicitud de expedición del Documento Nacional de Identidad y que contengan la anotación de que se ha emitido a los solos efectos de la obtención de este documento.

b) Una fotografía reciente en color del rostro del solicitante, tamaño 32 por 26 milímetros, con fondo uniforme blanco y liso, tomada de frente con la cabeza totalmente descubierta y sin gafas de cristales oscuros o cualquier otra prenda que pueda impedir o dificultar la identificación de la persona.

c) Certificado o volante de empadronamiento del Ayuntamiento donde el solicitante tenga su domicilio, expedido con una antelación máxima de tres meses a la fecha de la solicitud del documento nacional de identidad.

d) Los españoles residentes en el extranjero acreditarán el domicilio mediante certificación de la Representación Diplomática o Consular donde estén inscritos como residentes.

2. Excepcionalmente, en los supuestos en que, por circunstancias ajenas al solicitante, no pudiera ser presentado alguno de los documentos a que se refiere el apartado primero de este artículo, y siempre que se acrediten por otros medios, suficientes a juicio del responsable del órgano encargado de la expedición, los datos que consten en tales documentos, se le podrá expedir un Documento Nacional de Identidad con la validez que se indica en el artículo siguiente.

3. En el momento de la solicitud, al interesado se le recogerán las impresiones dactilares de los dedos índices de ambas manos. Si no fuere posible obtener la impresión dactilar de alguno de los dedos o de ambos, se sustituirá, en relación con la mano que corresponda, por otro dedo según el siguiente orden de prelación: medio, anular o pulgar; consignándose, en el lugar del soporte destinado a tal fin, el dedo utilizado, o la imposibilidad de obtener alguno de ellos.

**Artículo 6.** *Validez.*

1. Con carácter general el documento nacional de identidad tendrá un período de validez, a contar desde la fecha de la expedición o de cada una de sus renovaciones, de:

a) Dos años cuando el solicitante no haya cumplido los cinco años de edad.

b) Cinco años, cuando el titular haya cumplido los cinco años de edad y no haya alcanzado los treinta al momento de la expedición o renovación.

c) Diez años, cuando el titular haya cumplido los treinta y no haya alcanzado los setenta.

d) Permanente cuando el titular haya cumplido los setenta años.

2. De forma excepcional se podrá otorgar validez distinta al Documento Nacional de Identidad en los siguientes supuestos de expedición y renovación:

a) Permanente, a personas mayores de treinta años que acrediten la condición de gran inválido.

b) Por un año en los supuestos del apartado segundo del artículo 5 y del mismo apartado del artículo 7 siempre que, en éste último caso, no se puedan aportar los documentos justificativos que acrediten la variación de los datos.

3. No obstante lo dispuesto en este artículo, en cuanto a la validez de la utilidad informática prevista en el artículo 1.4 se estará a lo que específicamente se establece al respecto en el artículo 12 de este Real Decreto.

**Artículo 7.** *Renovación.*

1. Transcurrido el período de validez que para cada supuesto se contempla en el artículo anterior, el Documento Nacional de Identidad se considerará caducado y quedarán sin efecto las atribuciones y efectos que le reconoce el ordenamiento jurídico, estando su titular obligado a proceder a la renovación del mismo.

Dicha renovación se llevará a cabo mediante la presencia física del titular del Documento, que deberá abonar la tasa correspondiente y aportar una fotografía con las características señaladas en el artículo 5.1.b). También se le recogerán las impresiones dactilares que se refieren en el apartado tercero del mismo artículo.

2. Independientemente de los supuestos del apartado anterior se deberá proceder a la renovación del Documento Nacional de Identidad en los supuestos de variación de los datos que se recogen en el mismo, en cuyo caso será preciso aportar, además de lo establecido en el apartado anterior, los documentos justificativos que acrediten dicha variación.

**Artículo 8.** *Expedición de duplicados.*

1. El extravío, sustracción, destrucción o deterioro del Documento Nacional de Identidad, conllevará la obligación de su titular de proveerse inmediatamente de un duplicado, que será expedido en la forma y con los requisitos indicados para la renovación prevista en el apartado primero del artículo anterior. La validez de estos duplicados será la misma que tenían los Documentos a los que sustituyen, salvo que éstos se hallen dentro de los últimos 90 días de su vigencia, en cuyo caso se expedirán con la misma validez que si se tratara de una renovación.

2. Los documentos sustituidos perderán el carácter de Documento Nacional de Identidad, así como los efectos que el ordenamiento jurídico atribuye a éste con respecto a su titular.

**Artículo 9.** *Entrega del Documento Nacional de Identidad.*

1. La entrega del documento nacional de identidad deberá realizarse personalmente a su titular, y cuando éste sea menor de 14 años o sea una persona con capacidad judicialmente complementada, se llevará a cabo en presencia de quien tenga encomendada la patria potestad o tutela, o persona apoderada por estas últimas. En el momento de la entrega del documento nacional de identidad se proporcionará la información a que se refiere el artículo 18.b) de la Ley 59/2003, de 19 de diciembre.

2. La activación del certificado de firma electrónica en el documento nacional de identidad tendrá carácter voluntario y su utilización se realizará mediante una clave personal y secreta que el titular del documento nacional de identidad podrá introducir reservadamente en el sistema.

3. Al entregar el Documento renovado, se procederá a la retirada del anterior para su inutilización física. Una vez inutilizado podrá ser devuelto a su titular si éste lo solicita.

**Artículo 10.** *Características de la tarjeta soporte.*

1. El material, formato y diseño de la tarjeta soporte del Documento Nacional de Identidad se determinará por el Ministerio del Interior, teniendo en cuenta en su elaboración la utilización de procedimientos y productos conducentes a la consecución de condiciones de calidad e inalterabilidad y máximas garantías para impedir su falsificación. Llevará incorporado un chip electrónico al objeto de posibilitar la utilidad informática a que se refiere el artículo 1.4 de este Real Decreto.

2. La tarjeta soporte llevará estampados en el anverso, de forma destacada y preeminente los literales «Documento Nacional de Identidad», «España» y «Ministerio del Interior».

**Artículo 11.** *Contenido.*

1. El Documento Nacional de Identidad recogerá gráficamente los siguientes datos de su titular:

En el anverso:

Apellidos y nombre.
Fecha de nacimiento.
Sexo.
Nacionalidad.
Número personal del Documento Nacional de Identidad y carácter de verificación correspondiente al Número de Identificación Fiscal.
Fotografía.
Firma.

En el reverso:

Lugar de nacimiento.
Provincia-Nación.
Nombre de los padres.
Domicilio.
Lugar de domicilio.
Provincia.
Nación.
Caracteres OCR-B de lectura mecánica.

Los datos de filiación se reflejarán en los mismos términos en que consten en la certificación a la que se alude en el artículo 5.1.a) de este Real Decreto, excepto en el campo de caracteres OCR-B de lectura mecánica, en que por aplicación de acuerdos o convenios internacionales la transcripción literal de aquellos datos impida o dificulte la lectura mecánica y finalidad de aquellos caracteres.

2. Igualmente constarán los siguientes datos referentes al propio Documento y a la tarjeta soporte:

Fecha de caducidad
Número de soporte.

3. Los textos fijos se expresarán en castellano y los expedidos en territorio de aquellas Comunidades Autónomas que tengan otra lengua oficial, serán también expresados en esta.

4. El chip incorporado a la tarjeta soporte contendrá:

Datos de filiación del titular.
Imagen digitalizada de la fotografía.
Imagen digitalizada de la firma manuscrita.
Plantilla de la impresión dactilar del dedo índice de la mano derecha o, en su caso, del que corresponda según lo indicado en el artículo 5.3 de este Real Decreto.
Certificados reconocidos de autenticación y de firma, y certificado electrónico de la autoridad emisora, que contendrán sus respectivos períodos de validez.
Claves privadas necesarias para la activación de los certificados mencionados anteriormente.

**Artículo 12.** *Validez de los certificados electrónicos.*

1. Con independencia de lo que establece el artículo 6.1 sobre la validez del documento nacional de identidad, la vigencia de los certificados electrónicos reconocidos incorporados al mismo no podrá ser superior a cinco años.

A la extinción de la vigencia del certificado electrónico, podrá solicitarse la expedición de nuevos certificados reconocidos, manteniendo la misma tarjeta del Documento Nacional de Identidad mientras dicho Documento continúe vigente. Para la solicitud de un nuevo certificado deberá mediar la presencia física del titular en la forma y con los requisitos que se determinen por el Ministerio del Interior, de acuerdo con lo previsto en la Ley 59/2003, de 19 de diciembre.

2. El cumplimiento del período establecido en el apartado anterior implicará la inclusión de los certificados en la lista de certificados revocados que será mantenida por la Dirección General de la Policía, bien directamente o a través de las entidades a las que encomiende su gestión.

3. La pérdida de validez del Documento Nacional de Identidad llevará aparejada la pérdida de validez de los certificados reconocidos incorporados al mismo. La renovación del Documento Nacional de Identidad o la expedición de duplicados del mismo implicará, a su vez, la expedición de nuevos certificados electrónicos.

4. También serán causas de extinción de la vigencia del certificado reconocido las establecidas en la Ley 59/2003, de 19 de diciembre, que resulten de aplicación, y, entre otras, el fallecimiento del titular del Documento Nacional de Identidad electrónico.

5. En los supuestos previstos en el artículo 8.1 de este Real Decreto, el titular deberá comunicar inmediatamente tales hechos a la Dirección General de la Policía por los procedimientos y medios que al efecto habilite la misma, al objeto de su revocación.

**Artículo 13.** *Declaración de Prácticas y Políticas de Certificación.*

De acuerdo y en cumplimiento del artículo 19 de la Ley 59/2003, de 19 de diciembre, el Ministerio del Interior formulará una Declaración de Prácticas y Políticas de Certificación. Dicha Declaración de Prácticas y Políticas de Certificación estará disponible al público de manera permanente y fácilmente accesible en la página de Internet del Ministerio del Interior.

**Disposición adicional primera.** *Documento de sustitución del Documento Nacional de Identidad en supuestos de retirada de éste.*

En los supuestos en que, de acuerdo con las previsiones establecidas en las Leyes, sea acordada por la Autoridad competente la retirada temporal de Documento Nacional de Identidad por los órganos encargados de la expedición de éste, se procederá a dotar al interesado de un documento identificador que tendrá las características y funcionalidades que determine el Ministerio del Interior, atendiendo a las causas de su retirada.

**Disposición adicional segunda.** *Documento Nacional de Identidad de los menores de edad.*

La posesión del Documento Nacional de Identidad por los menores de edad no supone, por sí sola, autorización para desplazarse fuera del territorio nacional, debiendo ser suplida, a estos efectos, con la correspondiente autorización de quien ejerza la patria potestad o tutela.

**Disposición adicional tercera.** *Imposibilidad de expedición o renovación del Documento Nacional de Identidad.*

Cuando exista imposibilidad manifiesta para la expedición del Documento Nacional de Identidad, y sin perjuicio de que por las Autoridades y Órganos correspondientes se compruebe la personalidad del interesado por cualesquiera otros medios, excepcionalmente podrá sustituirse aquél por certificaciones anuales en las que consten los motivos de tal imposibilidad, que en los supuestos de renovación tendrán únicamente el fin de prorrogar la validez del Documento caducado.

**Disposición adicional cuarta.** *Remisión de información por vía telemática.*

1. La documentación requerida para la expedición del Documento Nacional de Identidad en el artículo 5.1 de este Real Decreto no será exigible cuando sea posible remitir ésta desde los órganos competentes por medios telemáticos a la Dirección General de la Policía, de conformidad con lo que se establezca mediante Convenio.

2. En estos casos, por Orden del Ministro del Interior se establecerá el régimen de aportación de dichos documentos.

**Disposición transitoria única.** *Validez de los Documentos Nacionales de Identidad expedidos o renovados de conformidad con la normativa anterior a este Real Decreto y proceso de sustitución.*

1. Los Documentos Nacionales de Identidad ya emitidos o los que se continúen expidiendo por el sistema anterior conforme a la normativa existente a la entrada en vigor de este Real Decreto seguirán siendo válidos y eficaces de conformidad con dicha normativa en tanto no se proceda a su sustitución por el Documento Nacional de Identidad de acuerdo con lo que se establece en el apartado siguiente de esta disposición.

2. La Dirección General de la Policía programará y organizará, temporal y territorialmente el proceso de sustitución de las tarjetas soporte del Documento Nacional de Identidad emitidas con anterioridad a la entrada en vigor de este Real Decreto por el nuevo Documento Nacional de Identidad, pudiendo establecerse por razones de interés público programaciones especiales para determinados colectivos.

3. Sólo se podrá solicitar la expedición del nuevo Documento Nacional de Identidad en el marco de la programación a que se hace referencia en el apartado anterior.

**Disposición derogatoria única.** *Derogación normativa.*

1. Quedan derogadas las siguientes disposiciones: Decreto 196/1976, de 6 de febrero, por el que se regula el Documento Nacional de Identidad, y las modificaciones llevadas a cabo en el mismo a través de los Reales Decretos 1189/1978, de 2 de junio; 2002/1979, de 20 de julio; 2091/1982, de 12 de agosto; y 1245/1985, de 17 de julio.

2. Asimismo, quedan derogadas todas aquellas normas de igual o inferior rango que se opongan a lo preceptuado en este Real Decreto.

**Disposición final primera.** *Título competencial.*

Este Real Decreto se dicta al amparo de las competencias atribuidas al Estado por el artículo 149.1.8.ª,18.ª, 21.ª y 29.ª de la Constitución.

**Disposición final segunda.** *Desarrollo.*

1. El Ministerio del Interior adoptará las disposiciones necesarias para dar cumplimiento a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, en materia de creación y modificación de ficheros de titularidad pública.

2. Se habilita a los Ministros del Interior, de Justicia, de Economía y Hacienda, de Industria, Turismo y Comercio y de Administraciones Públicas para que dicten, en el ámbito de sus respectivas competencias, cuantas disposiciones sean necesarias para el desarrollo y aplicación de este Real Decreto.

**Disposición final tercera.** *Tasas.*

El Gobierno promoverá la norma legal de rango adecuado para la adecuación de la tasa que haya de percibirse por la expedición del Documento Nacional de Identidad, de acuerdo con su coste y en consideración a los beneficios que proporciona a la comunidad.

**Disposición final cuarta.** *Entrada en vigor.*

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado», excepto lo relativo al artículo 1.4 que entrará en vigor cuando lo haga el nuevo formato y diseño del Documento Nacional de Identidad.

# § 49

## Orden ISM/189/2021, de 3 de marzo, por la que se regula el Registro electrónico de apoderamientos de la Seguridad Social

Ministerio de Inclusión, Seguridad Social y Migraciones
«BOE» núm. 55, de 5 de marzo de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-3421

Mediante la Orden ESS/486/2013, de 26 de marzo, por la que se crea y regula el Registro electrónico de apoderamientos de la Seguridad Social, para la realización de trámites y actuaciones por medios electrónicos, dicho registro se configura como medio para acreditar la representación otorgada a tal efecto a que se refiere el artículo 129.2 del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre.

Posteriormente, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, ha establecido una regulación completa y sistemática de las relaciones «ad extra» entre las administraciones públicas y los administrados, cuya finalidad principal es la simplificación y agilización de los procedimientos administrativos.

A este respecto, la referida Ley 39/2015, de 1 de octubre, dedica su título I a los interesados en el procedimiento, en el que, tras regular en su artículo 3 la capacidad de obrar para actuar ante las administraciones públicas a los efectos previstos en dicha ley, prevé en materia de representación nuevos instrumentos para su acreditación en el ámbito exclusivo de las administraciones públicas, regulando especialmente en sus artículos 5 y 6 el apoderamiento «apud acta», presencial o electrónico, y la acreditación de su inscripción en el registro electrónico de apoderamientos de la administración pública competente.

Por su parte, en el citado artículo 6 se establece la información mínima que deben contener los asientos que se realicen en los registros electrónicos de apoderamientos, ya sean generales o particulares, y se indica que los poderes que se inscriban en esos registros electrónicos deberán corresponder a alguna de las tres categorías siguientes:

En primer lugar, los poderes generales para que el apoderado pueda realizar en nombre del poderdante cualquier actuación administrativa y ante cualquier administración pública.

En segundo lugar, los poderes que permiten al apoderado actuar en nombre del poderdante para cualquier actuación administrativa ante una administración u organismo concreto.

En tercer lugar, los poderes que permiten al apoderado actuar en nombre del poderdante únicamente para la realización de determinados trámites especificados en el poder.

En este ámbito, el mismo artículo 6 de la Ley 39/2015, de 1 de octubre, prevé que los registros electrónicos generales de apoderamientos no impedirán la existencia de registros electrónicos particulares en cada organismo, donde se inscribirán los poderes otorgados

para la realización de actuaciones generales o trámites específicos ante el mismo. También prevé la interoperabilidad entre los registros electrónicos generales y particulares de apoderamientos a fin de constituir un instrumento válido de comprobación y acreditación de la representación de un tercero ante las administraciones públicas, bastando para ello no solo con la mera consulta electrónica de los datos contenidos en otros registros administrativos similares, sino también con la consulta al registro mercantil, al de la propiedad o al de los correspondientes protocolos notariales.

En atención a tales previsiones legales y en el marco del impulso al empleo de los medios electrónicos, informáticos y telemáticos en las relaciones entre la Administración de la Seguridad Social y los ciudadanos, mediante esta orden se procede a dar una nueva regulación al Registro electrónico de apoderamientos de la Seguridad Social, creado y regulado hasta este momento por la Orden ESS/486/2013, de 26 de marzo.

La nueva regulación del Registro electrónico de apoderamientos de la Seguridad Social viene motivada por la necesidad de desarrollar en dicho ámbito las previsiones que sobre la materia contiene la ya citada Ley 39/2015, de 1 de octubre, tanto en su artículo 5, acerca de los requisitos que han de cumplir los apoderamientos, en sus distintas modalidades, para poder ser inscritos en los registros electrónicos de las diferentes administraciones públicas, como en su artículo 6, respecto de la necesaria incorporación al referido Registro electrónico de los apoderamientos que se efectúen dentro de su ámbito competencial.

Esta orden se adecua a los principios de buena regulación previstos en el artículo 129 de la Ley 39/2015, de 1 de octubre.

Así, la norma es respetuosa con los principios de necesidad, eficacia y proporcionalidad, en tanto que con ella se persigue el fin pretendido, consistente en acomodar la regulación del Registro electrónico de apoderamientos de la Seguridad Social a las previsiones contenidas al respecto en la mencionada Ley 39/2015, de 1 de octubre, al objeto de asegurar la efectiva aplicación de lo establecido en este ámbito en sus artículos 5 y 6, no tratándose de una norma restrictiva de derechos, sino garante de los mismos.

Asimismo, su regulación cumple los principios de seguridad jurídica y eficiencia, al ser coherente con el resto del ordenamiento jurídico, estar sus objetivos claramente definidos y responder a la finalidad de mejorar el servicio público, al permitir a los interesados formalizar apoderamientos y acreditar representaciones en favor de terceros, no imponiéndoles nuevas cargas administrativas.

Finalmente, la orden se ajusta al principio de transparencia puesto que, de acuerdo con lo establecido en el artículo 26.6 de la Ley 50/1997, de 27 de noviembre, del Gobierno, se ha sometido al trámite de audiencia e información pública.

La orden ha sido informada favorablemente por la Comisión Ministerial de Administración Digital, conforme a lo establecido por el artículo 2.2.h) de la Orden ESS/1355/2015, de 25 de junio, por la que se creó dicho órgano colegiado en el entonces Ministerio de Empleo y Seguridad Social y se reguló su composición y funciones.

También ha sido informada por la Agencia Española de Protección de Datos, de acuerdo con lo previsto en el artículo 5.b) del Estatuto de la indicada Agencia, aprobado por el Real Decreto 428/1993, de 26 de marzo.

Esta orden se dicta en ejercicio de la habilitación conferida al Ministerio de Inclusión, Seguridad Social y Migraciones por el artículo 5.2.b) y la disposición final octava del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre, y de acuerdo con la competencia exclusiva en materia de legislación básica de la Seguridad Social que el artículo 149.1.17.ª de la Constitución Española atribuye al Estado.

En su virtud, con la aprobación previa de la Ministra de Política Territorial y Función Pública y de acuerdo con el Consejo de Estado, dispongo:

**Artículo 1.** *Objeto y ámbito de aplicación.*

1. Esta orden tiene por objeto regular los requisitos y condiciones de funcionamiento del Registro electrónico de apoderamientos de la Seguridad Social (en adelante el registro), en el que se inscribirán los apoderamientos que de forma voluntaria se otorguen «apud acta» a favor de un tercero, presencial o electrónicamente, por quien ostente la condición de

interesado en un procedimiento administrativo, para actuar en su nombre ante la Administración de la Seguridad Social.

2. El registro no tiene carácter público, será único en el ámbito de la Administración de la Seguridad Social y estará accesible en la sede electrónica de la Secretaría de Estado de la Seguridad Social y Pensiones (en adelante SEDESS).

3. Las representaciones legales no serán objeto de inscripción en el registro.

4. A los efectos de esta orden, se entiende por Administración de la Seguridad Social la totalidad de las direcciones generales, entidades gestoras y servicios comunes incluidos en el ámbito de aplicación de la SEDESS, de conformidad con el artículo 2.a) de la Orden TIN/1459/2010, de 28 de mayo, por la que se crea la sede electrónica de la Secretaría de Estado de la Seguridad Social.

**Artículo 2.** *Tipos de apoderamientos a inscribir en el registro.*

En el registro podrán inscribirse los siguientes tipos de apoderamientos:

a) Apoderamiento general, para que el apoderado pueda llevar a cabo en nombre del poderdante cualquier actuación administrativa en todas las materias, trámites y grupos de trámites recogidos en el anexo I, sin que se pueda renunciar o revocar el poder por separado respecto a alguno de ellos.

b) Apoderamiento por materias, para que el apoderado pueda actuar en nombre del poderdante y llevar a cabo cualquiera de los trámites y/o grupos de trámites en la materia seleccionada de entre las relacionadas en el anexo I, sin que se pueda renunciar o revocar el poder por separado respecto a alguno de estos trámites.

c) Apoderamiento por trámites y/o grupos de trámites, para que el apoderado pueda actuar en nombre del poderdante solo en aquellos trámites y/o grupos de trámites seleccionados de entre los relacionados en el anexo I, pudiéndose renunciar o revocar el poder por separado respecto a cualquiera de ellos.

**Artículo 3.** *Órganos competentes.*

1. Corresponde a la Secretaría de Estado de la Seguridad Social y Pensiones la titularidad y gestión del registro, así como la aprobación y modificación de los modelos que resulten precisos para su adecuada gestión.

2. Corresponde a la Gerencia de Informática de la Seguridad Social garantizar la disponibilidad y accesibilidad del registro; la identificación de los interesados mediante métodos de identificación admitidos en la SEDESS; la integridad de los datos incorporados; la generación de evidencias electrónicas que permitan la constatación de la fecha y hora de los accesos y actuaciones relevantes para la incorporación de tales datos, así como la generación de documentos electrónicos que acrediten los poderes inscritos en el registro.

**Artículo 4.** *Poderdantes y apoderados.*

1. Podrán otorgar apoderamiento las personas físicas, jurídicas y entidades sin personalidad jurídica que ostenten capacidad de obrar y que tengan la condición de interesados en relación con las materias, trámites y/o grupos de trámites relacionados en el anexo I.

2. Podrán ser apoderados las personas físicas que ostenten capacidad de obrar, así como las personas jurídicas cuando, además, tengan prevista en sus estatutos la posibilidad de actuar en representación de un tercero ante las administraciones públicas.

**Artículo 5.** *Apoderamientos. Otorgamiento y otras actuaciones.*

1. A efectos de su inscripción en el registro, los apoderamientos que se otorguen «apud acta» podrán efectuarse de las siguientes formas:

a) Mediante comparecencia electrónica en la SEDESS, a través del uso de los métodos de identificación y firma admitidos en ella.

Si el compareciente fuese una persona jurídica o una entidad sin personalidad jurídica, la identificación y firma se realizarán mediante el uso de certificados cualificados de

representante, como medio de acreditar la representación y capacidad para realizar las actuaciones en el registro.

b) Mediante comparecencia de la persona física en las oficinas de asistencia en materia de registros de la Seguridad Social, donde el compareciente, una vez identificado por el funcionario habilitado, firmará la correspondiente solicitud.

c) Mediante comparecencia de la persona física en las oficinas de asistencia en materia de registros de otras administraciones públicas u organismos, para la posterior remisión del poder al Registro electrónico de apoderamientos de la Seguridad Social.

2. La modificación de los datos y de la vigencia de los apoderamientos otorgados, así como la consulta sobre sus términos y situación y las demás actuaciones relativas a los mismos reguladas en esta orden, tales como su aceptación, renuncia y revocación, podrán llevarse a cabo, asimismo, en las formas señaladas en el apartado anterior.

**Artículo 6.** *Inscripción de los apoderamientos.*

1. El poderdante podrá solicitar la inscripción en el registro del apoderamiento otorgado en las formas previstas en el artículo 5.

2. Desde el registro se comunicará al apoderado el otorgamiento del poder a su favor, advirtiéndole, cuando proceda, de la necesidad de presentar la declaración responsable a que se refiere el apartado 4 de este artículo y de aceptar expresamente el apoderamiento en los supuestos a que se refiere el artículo 9.

A efectos de la comunicación indicada en el párrafo anterior, el poderdante deberá facilitar los datos de contacto del apoderado.

3. Los poderes surtirán efectos ante la Administración de la Seguridad Social desde la fecha de su inscripción en el registro y respecto de las materias, trámites y/o grupos de trámites a los que expresamente se refieran y que hayan sido seleccionados de entre los relacionados en el anexo I y publicados en la SEDESS.

4. Los poderes otorgados en favor de personas jurídicas no se inscribirán ni surtirán efecto hasta que aquellas procedan a presentar una declaración responsable manifestando que, en sus estatutos, está prevista la posibilidad de representar a terceros ante las administraciones públicas.

Esa declaración deberá firmarse electrónicamente en el plazo máximo de un mes a contar desde la presentación de la solicitud de inscripción del poder en el registro. En caso de presentarse nuevas solicitudes de registro de apoderamientos a favor de la misma persona jurídica, no será necesaria la presentación de una nueva declaración responsable, siempre y cuando se mantengan los requisitos de capacidad que la sustentan.

La declaración responsable sustituirá a la presentación de los estatutos, sin perjuicio de que estos puedan ser exigidos con posterioridad por el órgano, entidad gestora o servicio común competente. En este último caso deberá constar en el registro el resultado de la comprobación realizada.

5. Los apoderamientos que necesiten aceptación expresa por parte del apoderado no se inscribirán ni surtirán efecto hasta que se produzca dicha aceptación, en los términos señalados en el artículo 9.

**Artículo 7.** *Contenido del registro.*

1. El registro estará disponible en la SEDESS, donde se mantendrá una relación pública y actualizada de todas las materias, trámites y/o grupos de trámites competencia de la Administración de la Seguridad Social, que pueden ser objeto de apoderamiento.

2. En los asientos que se realicen para inscribir un apoderamiento en el registro se harán constar los siguientes datos:

a) Nombre y apellidos o denominación o razón social, documento nacional de identidad, número de identificación fiscal o documento equivalente del poderdante, así como sus datos de contacto.

b) Nombre y apellidos o denominación o razón social, documento nacional de identidad, número de identificación fiscal o documento equivalente del apoderado, así como sus datos de contacto.

c) Materias, trámites y/o grupos de trámites objeto de apoderamiento.

d) Periodo de vigencia del poder.
e) Número de referencia del poder asignado por el registro.
f) Fecha de inscripción en el registro.
g) Estado del poder.
h) Tipo de poder según las facultades que otorgue.

**Artículo 8.** *Plazo de vigencia de los apoderamientos inscritos en el registro.*

1. Los poderes inscritos en el registro tendrán una vigencia máxima de cinco años, a contar desde la fecha de su inscripción.
2. En cualquier momento antes de la finalización del plazo señalado en el apartado anterior el poderdante podrá modificar, revocar o prorrogar la vigencia del apoderamiento, en cuyo caso podrá solicitar la modificación de su plazo de vigencia en las formas previstas en el artículo 5.
3. Las prórrogas otorgadas por el poderdante tendrán una validez determinada, sin que esta pueda ser superior a cinco años contados desde la fecha de inscripción de la prórroga en el registro.

**Artículo 9.** *Aceptación expresa del apoderamiento.*

1. La aceptación expresa del apoderado resultará necesaria en los supuestos en los que el apoderamiento comprenda la recepción de comunicaciones o notificaciones, sea cual sea la naturaleza del procedimiento.
2. El apoderado deberá aceptar expresamente el apoderamiento en el plazo máximo de un mes desde su otorgamiento, en las formas previstas en el artículo 5.
En estos casos, el apoderamiento solo se inscribirá y surtirá efectos desde la fecha en que conste esa aceptación en el registro.

**Artículo 10.** *Renuncia y revocación del apoderamiento.*

La renuncia por el apoderado a un apoderamiento inscrito en el registro y la revocación de este por el poderdante, efectuadas en las formas previstas en el artículo 5, solo surtirán efectos desde la fecha en que se produzca la inscripción de la renuncia o la revocación en el registro.

**Artículo 11.** *Consulta al registro por parte de los interesados y obtención de certificados de poderes registrados.*

Los interesados podrán consultar de forma electrónica los datos relativos a la inscripción, contenido y vigencia del poder o poderes inscritos en los que figuren como poderdantes o apoderados, así como obtener certificados de los apoderamientos inscritos en el registro.

**Artículo 12.** *Protección de datos de carácter personal.*

En materia de protección de datos el registro se ajustará a lo previsto al respecto en la normativa española y europea directamente aplicable sobre protección de datos personales.

**Artículo 13.** *Aprobación de modelos.*

1. Se aprueban los siguientes modelos inscribibles en el registro, en función de los distintos tipos de apoderamientos a que se refiere el artículo 2 y de las actuaciones a realizar respecto a ellos:

a) Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante la Administración de la Seguridad Social de cualquier trámite en todas o en algunas de las materias relacionadas en el anexo I, y que figura como anexo II.
b) Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante la Administración de la Seguridad Social de determinados trámites, de entre los relacionados en el anexo I, y que figura como anexo III.
c) Aceptación, renuncia y revocación de poderes otorgados, que figura como anexo IV.
d) Modificación del plazo de vigencia, que figura como anexo V.

2. Cuando la comparecencia personal tenga lugar en las oficinas de asistencia en materia de registros de otra administración pública u organismo a que se refiere el artículo 5.1.c), los modelos indicados en el apartado anterior serán presentados en dicho registro para su envío, vía intercambio registral, a la Administración de la Seguridad Social, a efectos de su posterior inclusión en el Registro electrónico de apoderamientos de la Seguridad Social.

**Disposición adicional primera.** *Representación en el Sistema de remisión electrónica de datos en el ámbito de la Seguridad Social.*

La representación otorgada en el ámbito del Sistema de remisión electrónica de datos (Sistema RED) se regirá por su propia normativa.

**Disposición adicional segunda.** *Documentos normalizados de representación en materia de prestaciones.*

Los documentos normalizados de representación aprobados por las entidades gestoras al amparo del artículo 129.2 del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre, para su uso en los procedimientos dirigidos al reconocimiento de prestaciones de la Seguridad Social, seguirán siendo válidos, si bien no serán objeto de inscripción en el Registro electrónico de apoderamientos de la Seguridad Social.

**Disposición adicional tercera.** *No incremento de gasto público.*

Esta orden no implica incremento de dotaciones o retribuciones, ni de gasto de personal, ni de cualesquiera otros gastos a cargo del sector público. Asimismo, no supone disminución de ingreso alguno para la Hacienda Pública Estatal y se llevará a cabo con las disponibilidades presupuestarias existentes.

**Disposición transitoria única.** *Vigencia de anteriores apoderamientos.*

Los apoderamientos otorgados al amparo de la Orden ESS/486/2013, de 26 de marzo, por la que se crea y regula el Registro electrónico de apoderamientos de la Seguridad Social para la realización de trámites y actuaciones por medios electrónicos, perderán su validez el 2 de abril de 2021 si antes de esa fecha no han sido adaptados a la regulación de esta orden, mediante la cumplimentación de los nuevos modelos de poderes a que se refiere su artículo 13.

**Disposición derogatoria única.** *Derogación normativa.*

Queda derogada la Orden ESS/486/2013, de 26 de marzo, por la que se crea y regula el Registro electrónico de apoderamientos de la Seguridad Social para la realización de trámites y actuaciones por medios electrónicos.

**Disposición final primera.** *Título competencial.*

Esta orden se dicta al amparo de lo dispuesto en el artículo 149.1.17.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de legislación básica de la Seguridad Social.

**Disposición final segunda.** *Facultades de aplicación.*

Se habilita al titular de la Secretaría de Estado de la Seguridad Social y Pensiones para dictar cuantas resoluciones resulten necesarias para la aplicación y ejecución de lo previsto en esta orden y para actualizar sus anexos.

**Disposición final tercera.** *Entrada en vigor.*

La presente orden entrará en vigor el día 2 de abril de 2021.

## ANEXO I

### Relación de materias, trámites y grupos de trámites susceptibles de apoderamiento

| Materia | Trámites |
|---|---|
| Todas las gestiones con la Seguridad Social. | Todos los trámites con la Seguridad Social. |
| Prestaciones. | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. |
| | Recibir notificaciones y comunicaciones. |
| Inscripción, afiliación, cotización y recaudación. | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. |
| | Recibir notificaciones y comunicaciones. |
| Sanidad marítima. | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. |
| | Recibir notificaciones y comunicaciones. |
| Formación marítima y sanitaria. | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. |
| | Recibir notificaciones y comunicaciones. |
| Contratación. | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. |
| | Recibir notificaciones y comunicaciones. |
| Patrimonio. | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. |
| | Recibir notificaciones y comunicaciones. |
| Auditoría. | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. |
| | Recibir notificaciones y comunicaciones. |
| Reclamaciones y recursos. | Presentar reclamaciones y recursos, realizar alegaciones y recibir notificaciones o comunicaciones. |
| Procedimientos de la Dirección General de Ordenación de la Seguridad Social. | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. |
| | Recibir notificaciones y comunicaciones. |

| Materia | Descripción |
|---|---|
| Todas las gestiones con la Seguridad Social. | El apoderado podrá realizar todas las actuaciones en cualquier materia y trámite ante la Seguridad Social. |
| Prestaciones. | El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones de la Seguridad Social, incluidas las prestaciones específicas previstas para los trabajadores del mar, así como para su revalorización, revisión, mantenimiento y, en su caso, extinción.<br>Asimismo, podrá realizar todas esas actuaciones en relación con los procedimientos sancionadores en materia de prestaciones de la Seguridad Social. |
| Inscripción, afiliación, cotización y recaudación. | El apoderado podrá realizar actuaciones relativas a los procedimientos y servicios de inscripción, baja y variación de datos de las empresas en la Seguridad Social; el alta, baja y variación de datos de los trabajadores, así como la cotización y la recaudación de los recursos de la Seguridad Social, incluidas las actas de liquidación e infracción competencia de la Tesorería General de la Seguridad Social. |
| Sanidad marítima. | El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones y servicios relacionados con la sanidad preventiva y asistencial que realiza el Instituto Social de la Marina para el sector marítimo pesquero, como reconocimientos médicos de aptitud, inspección de las condiciones sanitarias de los buques, inspección de botiquines a bordo, ayudas para la dotación de botiquines, asistencia sanitaria a bordo y en el extranjero y vigilancia de la salud. |
| Formación marítima y sanitaria. | El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites relacionados con la formación profesional marítima y sanitaria prestada por el Instituto Social de la Marina. |
| Contratación. | El apoderado podrá realizar actuaciones relativas a los procedimientos relacionados con la contratación pública realizada por la Administración de la Seguridad Social. |
| Patrimonio. | El apoderado podrá realizar actuaciones y efectuar trámites relativos a los negocios patrimoniales con la Tesorería General de la Seguridad Social. |
| Auditoría. | El apoderado podrá realizar actuaciones en relación a las auditorías públicas que sobre las mutuas y las empresas colaboradoras con la Seguridad Social lleva a cabo la Intervención General de la Seguridad Social, así como respecto a las actuaciones de control financiero de ayudas y subvenciones realizadas por el citado órgano de control. |
| Reclamaciones y recursos. | El apoderado podrá realizar todos los trámites (presentación, alegaciones, prueba, desistimiento, etc.) y recibir las notificaciones y comunicaciones administrativas relativas a los recursos y reclamaciones formulados frente a actos dictados por la Administración de la Seguridad Social. |
| Procedimientos de la Dirección General de Ordenación de la Seguridad Social. | El apoderado podrá realizar todas las actuaciones relacionadas con los procedimientos competencia de la Dirección General de Ordenación de la Seguridad Social. |

| Trámite | Descripción |
|---|---|
| Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. | El apoderado puede presentar, subsanar o completar solicitudes, escritos, declaraciones y comunicaciones, acompañando, en su caso, los documentos acreditativos requeridos o que considere oportunos. También puede desistir de las solicitudes presentadas. Igualmente puede aportar a un procedimiento administrativo datos, documentos y elementos de prueba, formular alegaciones y, en su caso, participar en el trámite de audiencia.<br>Asimismo, puede realizar cualquier otro trámite o actuación administrativa prevista en la legislación aplicable, incluido el abono de una obligación o el cobro de una cantidad líquida. |
| Recibir notificaciones y comunicaciones. | El apoderado puede recibir las notificaciones de resolución o actos administrativos que ponen fin a los procedimientos o que implican efectos jurídicos y cuya fecha de recepción por parte del interesado marca el inicio del plazo para poder presentar reclamaciones o recursos.<br>Asimismo, puede recibir todas aquellas comunicaciones informativas, sin efectos jurídicos, que la entidad que gestiona el procedimiento pueda remitir al interesado. El apoderamiento de este trámite implica que las notificaciones y/o comunicaciones se realizarán por vía electrónica al apoderado, conforme a la regulación específica de dicha materia. |
| Presentar reclamaciones y recursos, realizar alegaciones y recibir notificaciones o comunicaciones. | El apoderado puede presentar escritos de reclamación y recursos contra resoluciones y actos de trámite en los casos legalmente previstos, intervenir en todos sus trámites, formular alegaciones y desistir de los mismos, así como recibir las notificaciones y comunicaciones que puedan generarse respecto a los recursos y reclamaciones formulados. |

## ANEXO II

**Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante la Administración de la Seguridad Social de cualquier trámite en todas o en algunas de las materias que se especifican**

Comparece el poderdante (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| | | |
|---|---|---|
| Nombre: | Primer apellido: | Segundo apellido: |
| DNI/NIF/Documento equivalente: | Teléfono: | Correo electrónico: |
| Domicilio: | | |
| Código Postal: | Localidad: | Provincia: |

☐ Persona jurídica o entidad sin personalidad jurídica que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| | | |
|---|---|---|
| **Identificación del representante:** | | |
| Nombre: | Primer apellido: | Segundo apellido: |
| DNI/NIF/Documento equivalente: | | |
| **Identificación de la persona jurídica:** | | |
| NIF: | Razón Social: | |
| Teléfono: | Correo electrónico: | |

**********

El poderdante otorga poder a favor de (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| | | |
|---|---|---|
| Nombre: | Primer apellido: | Segundo apellido: |
| DNI/NIF/Documento equivalente: | Correo electrónico: | |

☐ Persona jurídica que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| | |
|---|---|
| NIF: | Razón Social: |
| Correo electrónico: | |

**Poder**

**Tan amplio y bastante como en Derecho sea necesario para actuar en nombre del poderdante para la realización de cualquier trámite en las materias seleccionadas a continuación**

Elija una de las dos opciones siguientes:

☐ Materia general que abarca todas las gestiones con la Seguridad Social.

☐ Materia(s) concreta(s) incluidas en el ámbito de la Seguridad Social (elija una o varias opciones):

| | Materia | Descripción |
|---|---|---|
| ☐ | Prestaciones | El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones de la Seguridad Social, incluidas las prestaciones específicas previstas para los trabajadores del mar, así como para su revalorización, revisión, mantenimiento y, en su caso, extinción.<br>Asimismo, podrá realizar todas esas actuaciones en relación con los procedimientos sancionadores en materia de prestaciones de la Seguridad Social. |
| ☐ | Inscripción, afiliación, cotización y recaudación | El apoderado podrá realizar actuaciones relativas a los procedimientos y servicios de inscripción, baja y variación de datos de las empresas en la Seguridad Social; el alta, baja y variación de datos de los trabajadores, así como la cotización y la recaudación de los recursos de la Seguridad Social, incluidas las actas de liquidación e infracción competencia de la Tesorería General de la Seguridad Social. |
| ☐ | Sanidad marítima | El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones y servicios relacionados con la sanidad preventiva y asistencial que realiza el Instituto Social de la Marina para el sector marítimo pesquero, como reconocimientos médicos de aptitud, inspección de las condiciones sanitarias de los buques, inspección de botiquines a bordo, ayudas para la dotación de botiquines, asistencia sanitaria a bordo y en el extranjero y vigilancia de la salud. |
| ☐ | Formación marítima y sanitaria | El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites relacionados con la formación profesional marítima y sanitaria prestada por el Instituto Social de la Marina. |
| ☐ | Contratación | El apoderado podrá realizar actuaciones relativas a los procedimientos relacionados con la contratación pública realizada por la Administración de la Seguridad Social. |
| ☐ | Patrimonio | El apoderado podrá realizar actuaciones y efectuar trámites relativos a los negocios patrimoniales con la Tesorería General de la Seguridad Social. |
| ☐ | Auditoría | El apoderado podrá realizar actuaciones en relación a las auditorías públicas que sobre las mutuas y las empresas colaboradoras con la Seguridad Social lleva a cabo la Intervención General de la Seguridad Social, así como respecto a las actuaciones de control financiero de ayudas y subvenciones realizadas por el citado órgano de control. |
| ☐ | Reclamaciones y recursos | El apoderado podrá realizar todos los trámites (presentación, alegaciones, prueba, desistimiento, etc.) y recibir las notificaciones y comunicaciones administrativas relativas a los recursos y reclamaciones formulados frente a actos dictados por la Administración de la Seguridad Social. |
| ☐ | Procedimientos de la Dirección General de Ordenación de la Seguridad Social | El apoderado podrá realizar todas las actuaciones relacionadas con los procedimientos competencia de la Dirección General de Ordenación de la Seguridad Social. |

Vigencia del poder:

| | |
|---|---|
| Fecha de fin:<br>A rellenar por el poderdante<br><br>/ / | La vigencia máxima no podrá superar los cinco años a contar desde la fecha de la inscripción en el Registro electrónico de apoderamientos de la Seguridad Social. |

En _____, ____/____/____ Firma del poderdante:
Lugar Fecha

**ANEXO III**

**Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante la Administración de la Seguridad Social de determinados trámites**

Comparece el poderdante (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| | | |
|---|---|---|
| Nombre: | Primer apellido: | Segundo apellido: |
| DNI/NIF/Documento equivalente: | Teléfono: | Correo electrónico: |
| Domicilio: | | |
| Código Postal: | Localidad: | Provincia: |

☐ Persona jurídica o entidad sin personalidad jurídica que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| | | |
|---|---|---|
| **Identificación del representante:** | | |
| Nombre: | Primer apellido: | Segundo apellido: |
| DNI/NIF/Documento equivalente: | | |
| **Identificación de la persona jurídica:** | | |
| NIF: | Razón Social: | |
| Teléfono: | Correo electrónico: | |

**********

El poderdante otorga poder a favor de (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| | | |
|---|---|---|
| Nombre: | Primer apellido: | Segundo apellido: |
| DNI/NIF/Documento equivalente: | Correo electrónico: | |

☐ Persona jurídica que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| | |
|---|---|
| NIF: | Razón Social: |
| Correo electrónico: | |

**Poder**
**Tan amplio y bastante como en Derecho sea necesario para actuar en nombre del poderdante para la realización de los trámites seleccionados a continuación (elija una o varias opciones)**

| Materia* | Trámites* | |
|---|---|---|
| Prestaciones | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. | ☐ |
| | Recibir notificaciones y comunicaciones. | ☐ |
| Inscripción, afiliación, cotización y recaudación | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. | ☐ |
| | Recibir notificaciones y comunicaciones. | ☐ |
| Sanidad marítima | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. | ☐ |
| | Recibir notificaciones y comunicaciones. | ☐ |
| Formación marítima y sanitaria | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. | ☐ |
| | Recibir notificaciones y comunicaciones. | ☐ |
| Contratación | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. | ☐ |
| | Recibir notificaciones y comunicaciones. | ☐ |
| Patrimonio | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. | ☐ |
| | Recibir notificaciones y comunicaciones. | ☐ |
| Auditoría | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. | ☐ |
| | Recibir notificaciones y comunicaciones. | ☐ |
| Reclamaciones y recursos | Presentar reclamaciones y recursos, realizar alegaciones y recibir notificaciones o comunicaciones. | ☐ |
| Procedimientos de la Dirección General de Ordenación de la Seguridad Social | Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. | ☐ |
| | Recibir notificaciones y comunicaciones. | ☐ |

**NOTA: Consulte la descripción de materias y trámites al final de este formulario.*

Vigencia del poder:

| | |
|---|---|
| Fecha de fin:<br>A rellenar por el poderdante<br><br>/ / | La vigencia máxima no podrá superar los cinco años a contar desde la fecha de la inscripción en el Registro electrónico de apoderamientos de la Seguridad Social. |

En _____, ____/____/____ Firma del poderdante:
Lugar Fecha

| Materia | Descripción |
|---|---|
| Todas las gestiones con la Seguridad Social | El apoderado podrá realizar todas las actuaciones en cualquier materia y trámite ante la Seguridad Social. |
| Prestaciones | El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones de la Seguridad Social, incluidas las prestaciones específicas previstas para los trabajadores del mar, así como para su revalorización, revisión, mantenimiento y, en su caso, extinción.<br>Asimismo, podrá realizar todas esas actuaciones en relación con los procedimientos sancionadores en materia de prestaciones de la Seguridad Social. |
| Inscripción, afiliación, cotización y recaudación | El apoderado podrá realizar actuaciones relativas a los procedimientos y servicios de inscripción, baja y variación de datos de las empresas en la Seguridad Social; el alta, baja y variación de datos de los trabajadores, así como la cotización y la recaudación de los recursos de la Seguridad Social, incluidas las actas de liquidación e infracción competencia de la Tesorería General de la Seguridad Social. |
| Sanidad marítima | El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones y servicios relacionados con la sanidad preventiva y asistencial que realiza el Instituto Social de la Marina para el sector marítimo pesquero, como reconocimientos médicos de aptitud, inspección de las condiciones sanitarias de los buques, inspección de botiquines a bordo, ayudas para la dotación de botiquines, asistencia sanitaria a bordo y en el extranjero y vigilancia de la salud. |
| Formación marítima y sanitaria | El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites relacionados con la formación profesional marítima y sanitaria prestada por el Instituto Social de la Marina. |
| Contratación | El apoderado podrá realizar actuaciones relativas a los procedimientos relacionados con la contratación pública realizada por la Administración de la Seguridad Social. |
| Patrimonio | El apoderado podrá realizar actuaciones y efectuar trámites relativos a los negocios patrimoniales con la Tesorería General de la Seguridad Social. |
| Auditoría | El apoderado podrá realizar actuaciones en relación a las auditorías públicas que sobre las mutuas y las empresas colaboradoras con la Seguridad Social lleva a cabo la Intervención General de la Seguridad Social, así como respecto a las actuaciones de control financiero de ayudas y subvenciones realizadas por el citado órgano de control. |
| Reclamaciones y recursos | El apoderado podrá realizar todos los trámites (presentación, alegaciones, prueba, desistimiento, etc.) y recibir las notificaciones y comunicaciones administrativas relativas a los recursos y reclamaciones formulados frente a actos dictados por la Administración de la Seguridad Social. |
| Procedimientos de la Dirección General de Ordenación de la Seguridad Social | El apoderado podrá realizar todas las actuaciones relacionadas con los procedimientos competencia de la Dirección General de Ordenación de la Seguridad Social. |

| Trámites | Descripción |
|---|---|
| Presentar solicitudes, realizar alegaciones o aportar elementos de prueba | El apoderado puede presentar, subsanar o completar solicitudes, escritos, declaraciones y comunicaciones, acompañando, en su caso, los documentos acreditativos requeridos o que considere oportunos. También puede desistir de las solicitudes presentadas. Igualmente puede aportar a un procedimiento administrativo datos, documentos y elementos de prueba, formular alegaciones y, en su caso, participar en el trámite de audiencia.<br>Asimismo, puede realizar cualquier otro trámite o actuación administrativa prevista en la legislación aplicable, incluido el abono de una obligación o el cobro de una cantidad líquida. |
| Recibir notificaciones y comunicaciones | El apoderado puede recibir las notificaciones de resolución o actos administrativos que ponen fin a los procedimientos o que implican efectos jurídicos y cuya fecha de recepción por parte del interesado marca el inicio del plazo para poder presentar reclamaciones o recursos.<br>Asimismo, puede recibir todas aquellas comunicaciones informativas, sin efectos jurídicos, que la entidad que gestiona el procedimiento pueda remitir al interesado. El apoderamiento de este trámite implica que las notificaciones y/o comunicaciones se realizarán por vía electrónica al apoderado, conforme a la regulación específica de dicha materia. |
| Presentar reclamaciones y recursos, realizar alegaciones y recibir notificaciones o comunicaciones | El apoderado puede presentar escritos de reclamación y recursos contra resoluciones y actos de trámite en los casos legalmente previstos, intervenir en todos sus trámites, formular alegaciones y desistir de los mismos, así como recibir las notificaciones y comunicaciones que puedan generarse respecto a los recursos y reclamaciones formulados. |

**ANEXO IV**

**Aceptación, renuncia y revocación de poderes otorgados**

Elija solo una de las siguientes operaciones:

**Poderdante**

☐ Revocación de poder(es).

**Apoderado**

☐ Aceptación de poder(es).

☐ Renuncia de poder(es).

**********

Identificación del compareciente:

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| | | |
|---|---|---|
| Nombre: | Primer apellido: | Segundo apellido: |
| DNI/NIF/Documento equivalente: | | |

□ Persona jurídica o entidad sin personalidad jurídica -como poderdante- que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| | | |
|---|---|---|
| **Identificación del representante:** | | |
| Nombre: | Primer apellido: | Segundo apellido: |
| DNI/NIF/Documento equivalente: | | |
| **Identificación de la persona jurídica:** | | |
| NIF: | Razón Social: | |

**********

Indique a continuación los poderes afectados por la operación seleccionada separados por comas.

| |
|---|
| **Número de referencia de los poderes:** |

Efectos de la operación desde la fecha de inscripción
en el Registro electrónico de apoderamientos de la Seguridad Social.

En _____, ____/____/____ Firma del compareciente:

**ANEXO V**

**Modificación de plazo de poderes otorgados**

Comparece el poderdante (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| Nombre: | | Primer apellido: | Segundo apellido: |
|---|---|---|---|
| | DNI/NIF/Documento equivalente: | | |

☐ Persona jurídica o entidad sin personalidad jurídica -como poderdante- que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

| **Identificación del representante:** | | |
|---|---|---|
| Nombre: | Primer apellido: | Segundo apellido: |
| DNI/NIF/Documento equivalente: | | |
| **Identificación de la persona jurídica:** | | |
| NIF: | Razón Social: | |

**********

Indique a continuación los poderes afectados (una línea para cada poder).
La vigencia máxima no podrá superar los cinco años a contar desde la fecha de la inscripción en el Registro electrónico de apoderamientos de la Seguridad Social.

| **Número de referencia de los poderes:** | **Fecha de fin de los poderes (día/mes/año):** |
|---|---|
| | / / |
| | / / |
| | / / |
| | / / |
| | / / |
| | / / |
| | / / |
| | / / |

Efectos de la operación desde la fecha de inscripción
en el Registro electrónico de apoderamientos de la Seguridad Social.

En _____, ____/____/____ Firma del compareciente:

# § 50

## Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas

Ministerio de Política Territorial y Administración Pública
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13173

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas se desarrolla bajo lo establecido en el artículo 43 de la Ley 11/2007, de 22 de junio, y artículo 13 del Real Decreto 4/2010, de 8 de enero, para posibilitar la interconexión de las redes de las Administraciones públicas y permitir el intercambio de información entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros.

La Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas establece las condiciones en las que cualquier órgano de una Administración, o Entidad de Derecho Público vinculada o dependiente de aquélla, accederá a la Red SARA, y describe los roles y responsabilidades de los agentes que se conectan a la Red SARA así como los requisitos para la conexión, acceso y uso de los servicios que se prestan a través de aquélla.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

**Primero.**

Se aprueba la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas, cuyo texto se incluye a continuación.

**Segundo.**

La Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

## NORMA TÉCNICA DE INTEROPERABILIDAD DE REQUISITOS DE CONEXIÓN A LA RED DE COMUNICACIONES DE LAS ADMINISTRACIONES PÚBLICAS ESPAÑOLAS

### *I. Consideraciones generales*

I.1 *Objeto*.–La Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas tiene por objeto establecer las condiciones en las que cualquier órgano de una Administración, o Entidad de Derecho Público vinculada o dependiente de aquélla (en adelante, organización), accederá a la Red SARA.

I.2 *Ámbito de aplicación*.–El contenido de esta norma será de aplicación en la conexión a la Red SARA en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

### *II. Agentes y conexión a la Red SARA*

II.1 *Conexión a la Red SARA.*

1. El acceso a la Red SARA se realizará a través de lo que se denomina Punto de Presencia (PdP) entendido como cualquier sede en la que existe una conexión directa a la Red SARA, sin presencia de ninguna organización intermedia.

2. Entre los PdPs de la Red SARA podrán distinguirse los siguientes tipos:

a) Proveedores de Acceso a la Red SARA (PAS).

b) Centros de Proceso de Datos (CPD) de SARA.

c) Red sTESTA (secure Trans-European Services for Telematics between Administrations).

d) Centros externos de monitorización.

e) Prestadores de servicios de certificación.

f) Otros: como son las Ventanillas Únicas Empresariales.

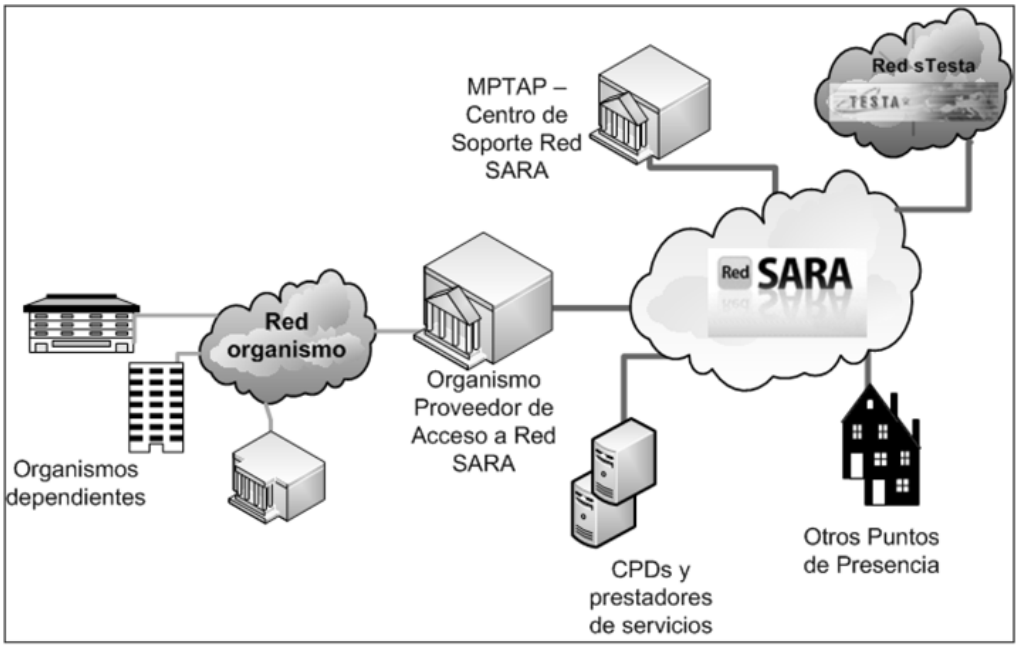



Figura 1. Puntos de Presencia y esquema de conexión a Red SARA

3. Con independencia de casos especiales de PdPs, en la conexión de cualquier organización a la Red SARA será necesaria la intervención del Ministerio de Política Territorial y Administración Pública (en adelante, MPTAP), un proveedor de acceso y la propia organización que desea conectarse, que actuará como usuario final.

II.2 *MPTAP-Centro de Soporte de la Red SARA.*–Las funcionalidades prestadas por el Centro de Soporte de la Red SARA del MPTAP se podrán consultar en el portal web www.redsara.es, accesible desde la Red SARA.

II.3 *Proveedores de Acceso a la Red SARA (PAS).*

1. La conexión directa a la Red SARA se proporcionará a través de un Área de Conexión (AC) que se ubicará en las dependencias de la Administración pública correspondiente convirtiéndose ésta en Proveedor de Acceso a la Red SARA (PAS) para sus Unidades, Organismos y Entidades de Derecho Público dependientes y, en el caso de las Comunidades Autónomas, también para las Administraciones Locales de su ámbito territorial.

2. Las organizaciones que no están adscritas a ningún organismo superior: Ministerios, Comunidades y ciudades con Estatuto de Autonomía y Órganos constitucionales, funcionarán como PAS a excepción de las Administraciones Locales que quedarán asignadas al PAS de la Comunidad Autónoma correspondiente.

3. Otros organismos públicos podrán asumir las funciones de PAS siempre que el MPTAP así lo establezca atendiendo a la singularidad del organismo o a la prestación, por parte de aquél, de servicios considerados singulares.

4. El establecimiento de un nuevo PAS, a solicitud del interesado, corresponderá al MPTAP a través del Centro de Soporte de la Red SARA.

II.4 *Órganos usuarios finales.*

1. Todo órgano usuario final de la Red SARA accederá a ésta a través de una organización que ejercerá las funciones de PAS.

2. Las características y dispositivos de la conexión de los órganos finales con el PAS correspondiente dependerán de las condiciones y mecanismos que disponga el propio PAS.

3. La solicitud de conexión de los órganos finales se dirigirá directamente al PAS del que dependen y será comunicada al Centro de Soporte de la Red SARA.

4. El listado completo de PAS estará disponible en el portal web www.redsara.es, accesible desde la Red SARA.

***III. Requisitos técnicos para la conexión del PAS***

III.1 *Esquema del Área de Conexión (AC).*

1. El AC de un PAS funcionará como punto único de conexión entre la red de la Administración pública correspondiente y sus organizaciones dependientes o asignadas al PAS, a las redes de otras administraciones y Entidades públicas conectadas a la Red SARA, así como a la Red sTESTA de la Comisión Europea.

2. La estructura del AC responderá al esquema de una zona desmilitarizada (DMZ) delimitada por un subsistema de seguridad externo, que conectará con el resto de la Red SARA, y un subsistema de seguridad interno hacia el interior de la organización.

3. Los elementos del AC, además de proporcionar seguridad perimetral, albergarán los servicios telemáticos básicos prestados por la Red SARA: DNS, SMTP, NTP, Proxy y Proxy inverso.

4. El subsistema de seguridad externo será el encargado de establecer una red privada virtual (VPN) hacia el resto de sedes de la Red SARA, con lo que todas las comunicaciones, a través del operador de servicios de telecomunicaciones, estarán cifradas mediante túneles.

5. En la zona intermedia, DMZ, será posible conectar cualquier equipo que la organización considere conveniente utilizar para la comunicación con el resto de organizaciones que componen la Red. Para no vulnerar la seguridad global de la Red, el Centro de Soporte de la Red SARA del MPTAP determinará las condiciones en que dichos elementos adicionales deberán integrarse en el AC.

6. Un esquema muy simplificado de un AC es el siguiente:

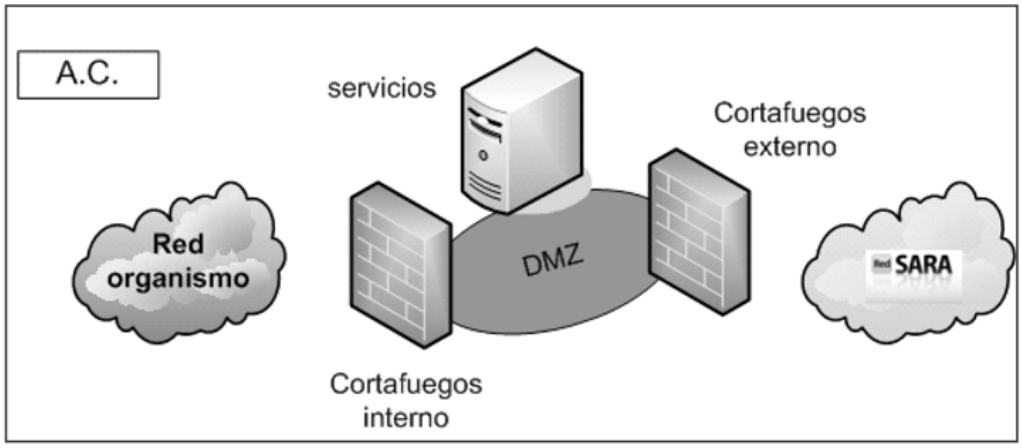



Figura 2. Esquema lógico de un Área de Conexión (AC)

III.2 *Administración de la conexión.*–El MPTAP administrará la conexión a la Red SARA y aplicará las políticas necesarias para el aseguramiento de la interoperabilidad y el nivel de seguridad correspondiente.

III.3 *Plan de direccionamiento.*

1. Las organizaciones que se conecten a la Red SARA aplicarán el Plan de direccionamiento e Interconexión de Redes en la Administración establecido por la Dirección General para el Impulso de la Administración Electrónica (DGIAE) disponible en http://administracionelectronica.gob.es/ según lo dispuesto en artículo 14 del Real Decreto 4/2010, de 8 de enero.

2. Todas las partes pondrán todos los medios a su alcance para adaptarse a los correspondientes planes de direccionamiento, de tal manera que un determinado rango o espacio de direcciones IP será reservado para preservar la compatibilidad e interoperabilidad.

III.4 *Dotación de elementos de conectividad.*–El MPTAP adquirirá, instalará, administrará, configurará y mantendrá los elementos de conectividad de cada PAS.

III.5 *Garantías de acondicionamiento físico.*–El acondicionamiento físico de las instalaciones del PAS cumplirá lo establecido a tal efecto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica de manera que se asegure la continuidad del servicio.

III.6 *Servicios de soporte y gestión de incidentes.*

1. El soporte y la gestión de incidentes de la Red SARA se prestarán de manera conjunta entre el MPTAP y los PAS, a través de sus correspondientes equipos dedicados a estos servicios.

2. Para facilitar la actuación conjunta entre el MPTAP y los PAS, cada organización proporcionará los siguientes datos de sus servicios de soporte y de gestión de incidentes:

a) Identificación.
b) Responsable de la unidad.
c) Responsable técnico.
d) Horario de servicio.
e) Localización.
f) Horario y datos de contacto para incidentes.
g) Observaciones.

3. Los datos identificativos y de contacto de los servicios de soporte y de gestión de incidentes de cada organización serán convenientemente actualizados y distribuidos entre todos los agentes de manera que se asegure la disponibilidad de la información de contacto para actuar ante cualquier incidente. Su consulta estará disponible a través del portal web www.redsara.es, accesible desde la Red SARA.

### *IV. Acceso y utilización de servicios*

IV.1 *Acceso a los servicios.*

1. Cualquier organización con conexión a la Red SARA, podrá solicitar la utilización de cualquiera de los servicios que se presten a través de ésta.

2. El catálogo de servicios disponibles en la Red SARA estará disponible en el portal web www.redsara.es, accesible desde la Red SARA.

IV.2 *Mantenimiento del catálogo de servicios.*

1. El catálogo de servicios será mantenido y actualizado por el MPTAP y el PAS a través del cual se presta cada servicio.

2. Todos los servicios que se publiquen en la Red SARA, a través de un PAS, serán comunicados al Centro de Soporte de la Red SARA con el fin de mantener el catálogo de servicios correctamente actualizado.

3. El catálogo de servicios facilitará la elaboración de estadísticas y cuadros de mando que el MPTAP podrá publicar en el portal web www.redsara.es y poner a disposición de todos los implicados.

IV.3 *Condiciones de utilización de los servicios.*

1. Para los servicios verticales o de negocio, así como para los servicios comunes de administración electrónica, con independencia de condiciones particulares que pudiese establecer el prestador del servicio, las condiciones de utilización serán

a) Acuerdo previo entre la Administración pública que presta el servicio y la beneficiaria.
b) Comunicación al Centro de Soporte de la Red SARA del MPTAP.
c) Si procede, condiciones de la plataforma de intermediación de datos que intervenga en el servicio. En caso de uso de la Plataforma de intermediación del MPTAP, se atenderá a lo establecido en la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos.

2. La solicitud de alta de un nuevo servicio y las comunicaciones al Centro de Soporte de la Red SARA se realizarán a través de los medios dispuestos para tal fin en el portal web www.redsara.es, donde figurarán, al menos, los siguientes datos:

a) Datos del solicitante.
b) Datos generales del servicio.

i. Nombre del servicio o aplicación.
ii. Nivel de criticidad.
iii. Horario de disponibilidad.
iv. Destinatarios del servicio.

c) Datos del soporte técnico para el contacto con dicho servicio.
d) Datos técnicos de acceso y uso del servicio.

***V. Agentes y roles***

V.1 *Ministerio de Política Territorial y Administración Pública.*–El MPTAP:

a) Instalará, administrará y mantendrá una conexión de capacidad suficiente y alta disponibilidad ubicada en las dependencias que la Administración pública determine y que mejor permita la conexión con su correspondiente red para constituirse como PAS.

b) Proporcionará a los responsables del PAS la documentación técnica correspondiente a la arquitectura y configuración de los sistemas que componen el AC.

c) Mantendrá un servicio de soporte 24x7 para garantizar la continuidad del servicio en el AC y la red troncal que sirva para realizar la gestión de incidentes y problemas, cuando le corresponda, así como la gestión de la resolución cuando intervengan agentes externos (fabricantes, operadores u otros organismos con acceso al sistema), consultas técnicas relacionadas con el servicio o peticiones de nuevos accesos.

d) Gestionará el portal web www.redsara.es, como espacio para facilitar información general sobre la Red SARA así como información específica para los responsables técnicos del PAS respecto del servicio proporcionado, notificación de incidencias, paradas programadas, publicación de nuevos servicios y otras informaciones de interés.

e) Adoptará las medidas de seguridad necesarias para proteger debidamente la información transmitida, mediante el cifrado de las comunicaciones y la detección temprana de incidentes en colaboración con el CCN-CERT.

V.2 *Proveedores de acceso a la Red SARA.*–Cualquier Administración pública que funcione como PAS:

a) Realizará las labores de conectividad y despliegue pertinentes para poder acceder desde sus propias dependencias o instalaciones a la Red SARA a través del AC.

b) Gestionará y mantendrá los elementos activos que conectan su red corporativa a la Red SARA.

c) Garantizará condiciones adecuadas en la ubicación del AC (condiciones medioambientales, suministro eléctrico, cableado, etc.) con el fin de asegurar la continuidad del servicio.

d) Mantendrá un servicio de soporte, a ser posible 24x7, para garantizar la continuidad del servicio en su función como PAS. Para ello se facilitarán al MPTAP los contactos, tanto de los responsables del PAS como los del Centro de Soporte, Centro de Atención al Usuario o equivalente.

e) Colaborará con el MPTAP en la gestión de incidentes y problemas, incluso si ello lleva consigo pequeñas comprobaciones o actuaciones en el AC, dirigidas desde el Centro de Soporte de la Red SARA, con el fin de reducir los tiempos de resolución de las incidencias que pudieran ocurrir.

f) Facilitará, promoverá y sostendrá el acceso a la Red SARA a sus Organismos y Entidades de Derecho Público dependientes y adicionalmente, en el caso de Comunidades Autónomas, a las Administraciones Locales de su ámbito territorial, con la tecnología, mecanismos y procedimientos que éstos acuerden, garantizando la continuidad del servicio y las condiciones adecuadas de seguridad en la parte que le corresponde.

g) Colaborará con el MPTAP en el mantenimiento del catálogo de servicios y conexiones.

V.3 *Órganos usuarios finales.*–Los Organismos y Entidades de Derecho Público dependientes y adicionalmente, en el caso de Comunidades Autónomas, las Administraciones Locales de su ámbito territorial, que disfruten del acceso a la Red SARA a través del PAS correspondiente, aplicarán:

a) Condiciones particulares del PAS del que dependen.
b) Condiciones particulares de servicios horizontales y verticales que utilizan a través de la Red SARA.

V.4 *Publicidad de referencias.*

1. El MPTAP podrá hacer pública, en cualquier lista de referencia o en cualquier boletín de prensa publicado y sin autorización previa, la relación de organismos usuarios de la Red SARA.
2. Las Administraciones públicas podrán referenciar la utilización de la Red SARA sin autorización previa por parte del MPTAP.

# § 51

## Resolución de 4 de julio de 2017, de la Secretaría de Estado de Función Pública, por la que se establecen las condiciones que han de cumplirse para tener la consideración de punto de presencia de la red SARA (PdP)

Ministerio de Hacienda y Función Pública
«BOE» núm. 162, de 8 de julio de 2017
Última modificación: sin modificaciones
Referencia: BOE-A-2017-8018

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, regula la Red SARA como la Red de comunicaciones que utilizarán preferentemente las Administraciones públicas españolas, para comunicarse entre sí, para lo cual conectarán a la misma, bien sus respectivas redes, bien sus nodos de interoperabilidad, de forma que se facilite el intercambio de información y de servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados miembros.

Señala el citado Real Decreto que para la conexión a la Red de comunicaciones de las Administraciones públicas españolas, serán de aplicación los requisitos previstos en la Norma Técnica de Interoperabilidad desarrollada conforme al procedimiento establecido en su disposición adicional primera.

Por Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, se aprueba la Norma Técnica de Interoperabilidad de requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas, en cuyo apartado II.1. Conexión a la Red SARA se establece que el acceso a la Red SARA se realizará a través de lo que se denomina Punto de Presencia (PdP) entendido como cualquier sede en la que exista una conexión directa a la Red SARA, sin presencia de ninguna organización intermedia.

La propia Norma establece los distintos tipos de PdPs de la Red SARA a considerar, clasificándolos en: Proveedores de Acceso a la Red SARA (PAS), Centros de Procesos de Datos (CPD) de SARA, Red sTESTA (secure Trans-European Services for Telematics between Administrations), Centros externos de monitorización, Prestadores de servicios de certificación y Otros.

Por Acuerdo de Consejo de Ministros de 2 de octubre de 2015 se aprueba el Plan de Transformación Digital de la Administración General del Estado y sus Organismos Públicos (Estrategia TIC 2015-2020), que constituye el marco estratégico global para avanzar en la transformación de la Administración, con el objetivo de que ésta sea capaz de adaptarse ágilmente a las nuevas demandas en un entorno cambiante con plenas garantías de seguridad, proporcionando información y servicios digitales de calidad, generando nuevas líneas de relación con los ciudadanos y facilitando la generación de oportunidades a nuestro tejido productivo a través de la innovación y desarrollo de las TIC.

En desarrollo de la Estrategia TIC y para el cumplimiento de las obligaciones que, en materia de administración digital, deben cumplir las Administraciones tras la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la Secretaría General de Administración Digital, ha desarrollado aplicaciones en nube que facilita su uso por las Administraciones, bien desde instalaciones propias o a través de las entidades privadas o públicas que les prestan servicio.

En este contexto, es preciso determinar las condiciones técnicas que han de cumplir las entidades privadas que prestan servicios de administración electrónica en la nube, a determinadas Administraciones para actuar como PdPs de la Red SARA preservando las máximas garantías de seguridad, confidencialidad y protección de datos.

Por este motivo, la Secretaría de Estado de Función Pública, en el ejercicio de las competencias que tiene atribuidas en desarrollo e impulso del proceso de racionalización de las TIC, así como la incorporación de las mismas a la prestación de los servicios públicos y la cooperación interadministrativa en esta materia, resuelve:

**Primero.**

Aprobar las condiciones específicas que deben cumplir las entidades privadas que facilitan servicios de administración electrónica, para ser consideradas PdP de la Red SARA, de acuerdo con lo dispuesto en el apartado II.1.2.f de la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de Comunicaciones de las Administraciones Públicas Españolas, y que se recogen en el anexo I.

**Segundo.**

Aprobar el procedimiento de solicitud de reconocimiento de la condición de PdP de la Red SARA, Anexo II.

**Tercero.**

Ordenar la publicación de esta Resolución, junto con sus anexos, en el «Boletín Oficial del Estado».

**Cuarto.**

La presente Resolución entra en vigor a partir del día siguiente a su publicación en el «Boletín Oficial del Estado».

## ANEXO I

### Condiciones para la adquisición de la condición de PdP de la Red SARA

Para poder adquirir la condición de PdP de la Red SARA es necesario el cumplimiento de los siguientes requisitos:

1. Que la empresa preste servicios de administración electrónica en la nube a Administraciones Públicas ubicadas en al menos dos Comunidades Autónomas.

2. Que cumpla con alguno de los siguientes criterios:

– Que de servicio al menos a 20 administraciones públicas, preferiblemente Entidades Locales.

– Que realice al menos 10.000 transacciones (1)/mes para las citadas Administraciones.

– Que al conjunto de Administraciones a las que preste servicio representen al menos a una población de 400.000 habitantes.

(1) Transacción: Interacción con una estructura de datos compleja. La transacción debe realizarse de una sola vez y sin que la estructura a medio manipular pueda ser alcanzada por el resto del sistema hasta que se hayan finalizado todos sus procesos.

3. Cumplimiento de los requisitos técnicos siguientes:

– Cumplimiento de todas las especificaciones establecidos en la «Norma Técnica de Interoperabilidad de Requisitos de Conexión a la Red de Comunicaciones de las Administraciones Públicas españolas, así como con las demás Normas Técnicas de Interoperabilidad, presentes o futuras, que puedan ser de aplicación en la prestación de los servicios.

– La Entidad que actúe como PdP asumirá cualquier responsabilidad derivada de su uso de la Red SARA y de sus servicios, especialmente en materia de seguridad y en lo relativo a las prescripciones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

– La Entidad que actúe como PdP asumirá la instalación de los elementos técnicos necesarios para la conectividad solicitada, así como para la prestación de los servicios que de ella se derivan, cuya provisión y activación será autorizada por la SGAD en los términos que determine.

– La Entidad que actúe como PdP se comprometerá a utilizar la conexión solicitada a los efectos exclusivos que se declaran en esta resolución.

– La Entidad que actúe como PdP deberá ejecutar satisfactoriamente las pruebas necesarias para garantizar el cumplimiento de sus funciones como PdP de la Red Sara y presentar documentación acreditativa de las mismas.

– La Entidad que actúe como PdP deberá comunicar a la Secretaría General de Administración Digital por los medios que, en cada caso, se habiliten a tales efectos:

• Los incidentes en la disponibilidad técnica de sus sistemas, en un plazo inferior a 1 hora.

• La baja definitiva en la prestación de sus servicios como prestador de servicio, con una anterioridad nunca inferior a dos meses.

• Las Entidades Usuarias a los que presta servicio.

– La Entidad Proveedora, informará periódicamente a la Secretaría General de Administración Digital, de cuantos datos sean requeridos en relación a la duración del acceso y la revisión de su estado y o bien condiciones.

4. La Secretaría de Estado de Función Pública resolverá en el plazo máximo de 1 mes. En la resolución se incluirán las condiciones relativas al deber de información periódica a la citada Secretaría de Estado, a través de la Secretaría General de Administración Digital, en adelante SGAD.

La Secretaría General de Administración Digital, adscrita a la Secretaria de Estado de Función Pública, con el fin de favorecer el despliegue de la Administración Digital y un uso adecuado de los recursos públicos podrá determinar, con el fin de ajustar los requisitos en función de la evolución de la demanda y del momento tecnológico, aplicando principios de transparencia, eficiencia y sostenibilidad del servicio, la modificación de estos criterios mediante instrucción de su titular.

## ANEXO II

### Procedimiento para la solicitud de reconocimiento de la condición de PdP de la Red SARA

1. La entidad interesada en tener la condición de PdP de la Red SARA dirigirá la solicitud a Secretaría General de la Administración Digital junto con la documentación acreditativa del cumplimiento de las condiciones recogidas en el Anexo I

2. Por resolución de la Secretaria de Estado de Función Pública. se reconocerá la condición de PdP de la Red SARA.

3. La condición de PdP se mantendrá en la medida que se cumpla con los requisitos exigidos en el Anexo I o los vigentes en el momento.

4. La solicitud electrónica, que comprenderá los contenidos referenciados en el anexo I, el correspondiente localizador uniforme de recursos (url), el contacto para dirigir dicha solicitud y la documentación acreditativa que debe acompañarse, se publicarán en el Portal de Administración Electrónica, en la ficha asociada al proyecto.

# § 52

## Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019, aprobada por el Consejo de Seguridad Nacional

Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad
«BOE» núm. 103, de 30 de abril de 2019
Última modificación: sin modificaciones
Referencia: BOE-A-2019-6347

El Consejo de Seguridad Nacional, en su reunión del día 12 de abril de 2019, ha aprobado la Estrategia Nacional de Ciberseguridad 2019.

Para general conocimiento se dispone su publicación en el «Boletín Oficial del Estado» como anexo a la presente Orden.

**ANEXO**

**Estrategia Nacional de Ciberseguridad 2019**

*Sumario*

**Resumen ejecutivo**

La Estrategia Nacional de Ciberseguridad desarrolla las previsiones de la Estrategia de Seguridad Nacional de 2017 en el ámbito de la ciberseguridad, considerando los objetivos generales, el objetivo del ámbito y las líneas de acción establecidas para conseguirlo.

El documento se estructura en cinco capítulos. El primero, titulado «El ciberespacio, más allá de un espacio común global», proporciona una visión de conjunto del ámbito de la ciberseguridad, los avances realizados en materia la materia desde la aprobación de la Estrategia de 2013, las razones que afianzan la elaboración de la Estrategia Nacional de Ciberseguridad 2019, así como las principales características que impulsan su desarrollo.

Las actividades que se desarrollan en el ciberespacio son fundamentales para la sociedad actual. La tecnología e infraestructuras que forman parte del ciberespacio son elementos estratégicos, transversales a todos los ámbitos de actividad, siendo la vulnerabilidad del ciberespacio una de los principales riesgos para nuestro desarrollo como nación.

Por ello, la seguridad en el ciberespacio es un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su Seguridad Nacional y una competencia del Estado para crear una sociedad digital en la que la confianza es un elemento fundamental.

Contribuir a la promoción de un ciberespacio seguro y fiable, desde un enfoque multidisciplinar abarcando aspectos más allá de los puramente técnicos, es una tarea que debe partir del conocimiento y comprensión de las amenazas a las que nos podemos enfrentar, incluyendo nuevas y emergentes.

El segundo capítulo, titulado «Las amenazas y desafíos en el ciberespacio» determina las principales amenazas del ciberespacio que derivan de su condición de espacio global común, de la elevada tecnificación y de la gran conectividad que posibilita la amplificación del impacto ante cualquier ataque. Clasifica estas amenazas y desafíos en dos categorías: por un lado, las que amenazan a activos que forman parte del ciberespacio; y por otro, aquellos que usan el ciberespacio como medio para realizar actividades maliciosas e ilícitas de todo tipo.

El tercer capítulo, titulado «Propósito, principios y objetivos para la ciberseguridad» aplica los principios rectores de la Estrategia de Seguridad Nacional 2017 (Unidad de acción, Anticipación, Eficiencia y Resiliencia) a cinco objetivos específicos. Su desarrollo, se plasma en el cuarto capítulo titulado «Líneas de acción y medidas», donde se establecen siete líneas de acción y se identifican las medidas para el desarrollo de cada una de ellas.

Dichas líneas de acción se dirigen a: reforzar las capacidades ante las amenazas provenientes del ciberespacio; garantizar la seguridad y resiliencia de los activos estratégicos para España; impulsar la ciberseguridad de ciudadanos y empresas; reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio;

impulsar la ciberseguridad de ciudadanos y empresas; potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital; contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable en apoyo de los intereses nacionales y desarrollar una cultura de ciberseguridad de manera que se contribuya al Plan Integral de Cultura de Seguridad Nacional.

El quinto capítulo, titulado «La ciberseguridad en el Sistema de Seguridad Nacional» define la arquitectura orgánica de la ciberseguridad. Bajo la dirección del Presidente del Gobierno, la estructura se compone de tres órganos: el Consejo de Seguridad Nacional, como Comisión Delegada del Gobierno para la Seguridad Nacional; el Consejo Nacional de Ciberseguridad, que apoya al Consejo de Seguridad Nacional y asiste al Presidente del Gobierno en la dirección y coordinación de la política de Seguridad Nacional en el ámbito de la ciberseguridad, y fomenta las relaciones de coordinación, colaboración y cooperación entre Administraciones Públicas y entre estas y el sector privado, y el Comité de Situación que, con el apoyo del Departamento de Seguridad Nacional, apoyará a la gestión de las situaciones de crisis en cualquier ámbito, que por su transversalidad o dimensión, desborden las capacidades de respuesta de los mecanismos habituales.

Se complementa este sistema con la Comisión Permanente de Ciberseguridad, que facilita la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad, siendo el órgano que asistirá al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad; las autoridades públicas competentes y CSIRT (Computer Security Incident Response Team) de referencia nacional, y se incorpora la creación de un elemento novedoso de colaboración público privada, el foro Nacional de Ciberseguridad.

Asimismo, en este último capítulo, se exponen a modo de conclusión, unas consideraciones finales y se concretan los mecanismos para la actualización y evaluación de la Estrategia.

**Introducción**

La Estrategia Nacional de Ciberseguridad 2019 establece la posición de España ante una nueva concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional.

En 2013 se aprobó la primera Estrategia Nacional de Ciberseguridad en España. El documento fijaba las directrices y líneas generales de actuación para hacer frente al desafío que supone, para el país, la vulnerabilidad del ciberespacio. Además, la estrategia diseñaba el modelo de gobernanza para la ciberseguridad nacional. Igualmente, en estos años, España ha seguido avanzando en sus esfuerzos por contribuir a la promoción de un ciberespacio seguro y fiable.

Uno de sus pilares, creado en el año 2014, es el Consejo Nacional de Ciberseguridad, órgano de apoyo del Consejo de Seguridad Nacional. Desde su primera reunión, el Consejo Nacional de Ciberseguridad ha asumido la tarea de coordinar los organismos con competencia en la materia a nivel nacional y el desarrollo del Plan Nacional de Ciberseguridad y sus planes derivados. Así, hoy España cuenta con organismos especializados en ciberseguridad y una posición destacada a nivel europeo e internacional.

El marco jurídico también ha experimentado una notable adaptación. En respuesta a su evolución y a la experiencia acumulada en estos años, en 2015 se publicó la modificación del Esquema Nacional de Seguridad para garantizar la seguridad de los sistemas del Sector Público. Por otro lado, la entrada en vigor del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone al ordenamiento jurídico español la Directiva (UE) 2016/1148 (conocida como Directiva NIS), ha supuesto un importante hito en la mejora de la ciberseguridad en nuestro país, extendiendo el alcance de esta Directiva con el objetivo de mejorar la ciberseguridad de todos los sectores estratégicos.

La Ley 36/2015, de 28 de septiembre, de Seguridad Nacional se promulgó con vocación de dar impulso a uno de los proyectos de mayor responsabilidad para un gobierno, la Seguridad Nacional. La Ley de Seguridad Nacional contempla la ciberseguridad como ámbito de especial interés.

Se puede afirmar, sin lugar a dudas, que la ciberseguridad ha modernizado la Seguridad Nacional, tratándose de uno de los ámbitos de mayor avance hasta la fecha. Esta dinámica debe seguir su camino adelante.

La Estrategia de Seguridad Nacional 2017 marca un punto de inflexión en el pensamiento estratégico nacional, donde la ciberseguridad debe ocupar un espacio propio y diferencial.

Una de las tendencias globales identificadas en la Estrategia, la digitalización, se muestra como motor del cambio con implicaciones para la seguridad. La Estrategia establece un esquema novedoso, con cinco objetivos generales que resultan transversales a todos los ámbitos. La gestión de crisis, la cultura de Seguridad Nacional, los espacios comunes globales, el desarrollo tecnológico y la proyección internacional de España conforman una matriz estratégica donde la ciberseguridad está llamada a abrir nuevas vías hacia el modelo de presente y futuro de la seguridad en España.

La nueva ciberseguridad se extiende más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social.

Además de las acciones para causar efectos en los sistemas digitales, se debe tener en cuenta la concepción del ciberespacio como un vector de comunicación estratégica, que puede ser utilizado para influir en la opinión pública y en la forma de pensar de las personas a través de la manipulación de la información, las campañas de desinformación o las acciones de carácter híbrido. Su potencial aplicación en situaciones muy diversas, donde se incluyen los procesos electorales, genera un elevado grado de complejidad.

Ante esta visión renovada de un ámbito que se entiende extendido funcionalmente, y para el que la colaboración público-privada es un elemento clave, resulta necesaria una nueva aproximación, una nueva estrategia nacional de ciberseguridad.

## CAPÍTULO 1

### El ciberespacio como espacio común global

Este capítulo presenta las oportunidades y desafíos del ciberespacio y la infraestructura digital, expone el carácter inherentemente internacional de la aproximación a su seguridad y describe los principales rasgos de la nueva concepción de la ciberseguridad en España.

El ciberespacio: oportunidades y desafíos:

El ciberespacio es un espacio común global caracterizado por su apertura funcional y su dinamismo. La ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones que en él se desarrollan definen un escenario que ofrece innumerables oportunidades de futuro, aunque también presenta serios desafíos a la seguridad.

Por una parte, el ciberespacio posibilita la conectividad universal y facilita el libre flujo de información, servicios e ideas. Se constituye así en un ámbito que estimula el emprendimiento, potencia el progreso socioeconómico y ofrece cada día nuevas posibilidades en todos los sectores de actividad. El cambio que la transformación digital provoca en los procesos productivos se manifiesta a escala global y a un ritmo sin precedentes. La inteligencia artificial, la robótica, el big data, el blockchain y el internet de las cosas son ya una realidad, si bien el verdadero potencial transformador está todavía por descubrir. Sus implicaciones van más allá de la dimensión tecnológica, se extienden hacia nuevos modelos sociales y se adentran en el campo de las relaciones personales y la ética.

Por otra parte, la digitalización transforma la seguridad y presenta serios desafíos. El ciberespacio se configura como campo de batalla donde la información y la privacidad de los datos son activos de alto valor en un entorno de mayor competición geopolítica, reordenación del poder y empoderamiento del individuo. Así, la creciente conectividad y la mayor dependencia de las redes y sistemas, así como de componentes, objetos y dispositivos digitales, generan vulnerabilidades y dificultan la adecuada protección de la información.

Infraestructura digital:

Además de su naturaleza virtual, el ciberespacio se sustenta en elementos físicos y lógicos. Los dispositivos, componentes y sistemas que constituyen las redes y sistemas de información y comunicaciones están expuestos a disfunciones que alteran su correcto funcionamiento y a acciones deliberadas con fines malintencionados, que ponen en riesgo el funcionamiento de las infraestructuras críticas y de los servicios esenciales que dependen de los sistemas y redes digitales asociadas.

Este riesgo se ve amplificado por la prevalencia de criterios comerciales frente a los de seguridad en el diseño de los productos hardware y software, así como de los sistemas y de los servicios, algo que dificulta los procesos de certificación y puede comprometer la cadena de suministro.

Todos estos elementos, unidos a la creciente interconectividad entre sistemas pueden originar efectos en cascada con resultados impredecibles.

Plano internacional: seguridad en el ciberespacio:

La seguridad en el ciberespacio se ha convertido en un objetivo prioritario en las agendas de los gobiernos con el fin de garantizar su seguridad nacional y de crear una sociedad digital basada en la confianza. En este contexto, España defiende su visión e intereses como nación y contribuye al esfuerzo conjunto de la comunidad internacional en su apuesta por un ciberespacio abierto, plural y seguro.

España continúa participando activamente en todas las instituciones en las que la ciberseguridad ocupa un lugar destacado, en especial en el marco de la Unión Europea, la Alianza Atlántica y de Naciones Unidas, demostrando así el compromiso con sus socios y aliados. Asimismo, se mantienen vínculos con terceros Estados mediante mecanismos de cooperación bilateral que facilitan elementos de entendimiento y confianza mutua basados en las relaciones fluidas en el ámbito de la ciberseguridad y orientados hacia la construcción de capacidades.

Consciente de la importancia del multilateralismo, además del Derecho Internacional y las normas no vinculantes de comportamiento responsable de los Estados, se destaca el papel de La Carta de Naciones Unidas como principio de referencia para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio. La construcción de consensos y las medidas de fomento de confianza constituyen la base para su aplicación y puesta en práctica, así como los Tratados y Convenios Internacionales en los que España es parte.

Una nueva concepción del ciberespacio:

Es una dimensión fundamental para la estabilidad el preservar la defensa de los valores y principios constitucionales y democráticos, así como los derechos fundamentales de los ciudadanos en el ciberespacio, especialmente en la protección de sus datos personales, su privacidad, su libertad de expresión y el acceso a una información veraz y de calidad.

El buen entendimiento de este planteamiento, exige trabajar con un enfoque multidisciplinar que abarque aspectos más allá de los puramente técnicos, bajo el principio de dirección centralizada y ejecución coordinada, con la afectación de la ciberseguridad a la Seguridad Nacional como competencia del Estado.

En primer lugar, el sector privado juega un papel relevante como uno de los gestores y propietarios de los activos digitales de España, por lo que las capacidades de ciberseguridad del país residen en gran medida en las de sus empresas. Es por tanto necesario el apoyo, la promoción y la inversión en ciberseguridad para impulsar la competitividad y el crecimiento económico, a la vez que proporcionar un entorno digital seguro y fiable.

Por otra parte, se debe aspirar a incrementar la autonomía tecnológica mediante el fomento de una base industrial nacional de ciberseguridad, la I+D+i y la gestión del talento tecnológico. En efecto, el recurso humano continúa siendo un factor crítico. Existe una diferencia importante entre el número de puestos de trabajo para los que es necesaria una alta especialización en las tecnologías de la información, en concreto en ciberseguridad, y las personas disponibles con el nivel de conocimiento o de formación requerida.

En segundo lugar, la transición de un modelo de ciberseguridad de carácter preventivo y defensivo hacia un esquema que incorpore elementos de mayor fuerza disuasoria obedece a un contexto global de mayor competencia geopolítica. El empleo del ciberespacio como dominio de confrontación, de forma independiente o como parte de una acción híbrida, es un

rasgo ampliamente reconocido. La disuasión en ciberseguridad requiere la obtención y potenciación de capacidades de ciberdefensa, como elemento fundamental de la acción del Estado.

En tercer lugar, la rápida evolución de las ciberamenazas aconseja una aproximación más proactiva de la ciberinteligencia. Su integración en el esquema conjunto de la ciberseguridad es un elemento clave para el conocimiento de la situación y la necesaria alerta temprana que permita anticiparse a las acciones de los potenciales adversarios a través del conocimiento de sus capacidades, técnicas, tácticas e intenciones. Así mismo, es necesario fomentar el empleo de mecanismos y medios que permitan una oportuna investigación y persecución de los autores para incrementar las posibilidades de atribución.

A todo lo anterior se une la necesidad de una mayor implicación de toda la sociedad mediante el fomento de una cultura de ciberseguridad, para evolucionar desde la concienciación al compromiso, en el entendimiento de que el ciudadano es corresponsable de la ciberseguridad nacional.

## CAPÍTULO 2

### Las amenazas y desafíos en el ciberespacio

En este capítulo se examinan las principales amenazas y desafíos del ciberespacio a los que se enfrenta España.

La promoción de un entorno seguro y fiable es una tarea que debe partir del conocimiento y la comprensión de los desafíos y las amenazas, incluyendo las nuevas y emergentes que afectan al ciberespacio. La Estrategia de Seguridad Nacional de 2017 diferencia entre las ciberamenazas y las acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas.

Ciberamenazas:

Las ciberamenazas son todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos. Abarcan un amplio abanico de acciones. Las ciberamenazas se caracterizan por su diversidad tanto en lo que concierne a capacidades como a motivaciones. Afectan a la práctica totalidad de los ámbitos de la Seguridad Nacional, como la Defensa Nacional, la seguridad económica o la protección de las infraestructuras críticas, entre otros, y no distinguen fronteras.

Su carácter transversal, exige que la ciberseguridad sea afrontada con una perspectiva integral que comprenda a las Administraciones Públicas, al sector público y privado y a la sociedad en su conjunto, en tanto puede tener implicaciones simultáneas en aspectos tan diversos como la soberanía, los derechos fundamentales, la defensa, la economía y el desarrollo tecnológico.

En este escenario, las defensas deben evolucionar continuamente para ir adaptándose a una amenaza que lleva la iniciativa y que se multiplica por el efecto llamada que genera su alto grado de impunidad. Todo ello, mientras la superficie a defender se incrementa y complica cada día.

En este sentido, la seguridad de las redes y sistemas de información requiere potenciar las medidas de prevención, detección y respuesta, fomentando la seguridad por diseño y por defecto, que debe estar incorporada tanto en el desarrollo de productos y servicios tecnológicos, como en su actualización o manera de utilización.

Acciones que usan el ciberespacio para fines maliciosos:

Las tecnologías digitales dan entrada a nuevas actividades y formas de negocio que requieren ser debidamente reguladas, pues pueden afectar a la estabilidad y al ejercicio de derechos y libertades, presentando sustanciales amenazas y desafíos para la Seguridad Nacional. Igualmente, las mismas cualidades que hacen del ciberespacio un motor del progreso, pueden ser explotadas con fines perniciosos al sumarse a las excepcionales facilidades que concede para el anonimato, la suplantación y la amplificación.

Debido a la revolución de Internet, Estados, grupos organizados, colectivos y hasta individuos aislados pueden alcanzar un nivel de poder y una capacidad de influir impensable

en otros tiempos. La conectividad digital lleva a que los movimientos sociales globales tengan una importancia estratégica hasta hace poco subestimada.

Las acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas incluyen las relacionadas con el ciberespionaje y la cibercriminalidad.

El ciberespionaje es un método relativamente económico, rápido y con menos riesgos que el espionaje tradicional, dada la dificultad de atribución de la autoría. Las mayores capacidades corresponden principalmente a actores estatales (organismos de inteligencia o militares), que fundamentalmente operan a través de las denominadas Amenazas Persistentes Avanzadas (APT). Un tipo de amenaza en la que el adversario posee sofisticados niveles de conocimiento y de recursos e infraestructuras para, mediante múltiples tipos de ataques, interactuar sobre sus objetivos por un extenso periodo de tiempo, adaptarse a los esfuerzos del defensor para resistir, así como mantener el nivel de interacción para ejecutar sus objetivos.

Asimismo, se constata una tendencia creciente de las denominadas amenazas híbridas, acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los estados democráticos y las instituciones, a través de una amplia gama de medios, tales como acciones militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica. Actores estatales y no estatales, bien de forma directa o a través de intermediarios, explotan las facilidades que ofrece Internet para la desinformación y propaganda y un interés generalizado en la obtención y desarrollo de capacidades militares para operar en el ciberespacio, incluyendo en muchos casos capacidades ofensivas.

La cibercriminalidad, por su parte, es un problema de seguridad ciudadana de primer orden, representando una de las amenazas más extendidas y generalizadas, que se materializa de forma continua y que victimiza cada vez de manera más importante a miles de instituciones, empresas y ciudadanos. El término Cibercriminalidad, hace referencia al conjunto de actividades ilícitas cometidas en el ciberespacio que tienen por objeto los elementos, sistemas informáticos o cualesquiera otros bienes jurídicos, siempre que en su planificación, desarrollo y ejecución resulte determinante la utilización de herramientas tecnológicas; en función de la naturaleza del hecho punible en sí, de la autoría, de su motivación, o de los daños infligidos, se podrá hablar así de ciberterrorismo, de ciberdelito, o en su caso, de hacktivismo.

El empleo de nuevas modalidades de transacción financiera y económica, como las criptomonedas, para el tráfico y el comercio de bienes y prestación de servicios ilícitos o la extorsión, el fraude y la falsificación de medios de pago no monetarios, constituyen un serio desafío a la seguridad por su sofisticación y complejidad. Estos pueden ser utilizados en el blanqueo de capitales y la evasión de impuestos y representan una fuente de ingresos para el crimen organizado y por lo tanto son facilitadores de otras actividades como la financiación del terrorismo, que toma provecho de la dificultad de seguimiento que estas nuevas técnicas ofrecen.

Los ciberdelincuentes operan bajo esquemas de crimen organizado y continúan explorando de manera incesante técnicas sobre las que construir modelos de negocio lucrativo y de bajo riesgo, amparados por la difícil trazabilidad de sus acciones.

Los grupos terroristas tratan de aprovechar las vulnerabilidades del ciberespacio para realizar ciberataques o para actividades de radicalización de individuos y colectivos, financiación, divulgación de técnicas y herramientas para la comisión de atentados, y de reclutamiento, adiestramiento o propaganda. Íntimamente relacionado con ello, se halla la amenaza contra las infraestructuras críticas, con la posibilidad cierta de causar un colapso a través de las redes mediante una caída en cadena de los servicios esenciales.

Los grupos hacktivistas realizan ciberataques por razones ideológicas y, aprovechándose en ocasiones de productos, servicios y herramientas disponibles en el ciberespacio, buscan desarrollar ataques con un gran impacto mediático o social.

Tampoco se puede menospreciar la amenaza que entraña el incremento continuado de la contratación de servicios de cibercriminales, las organizaciones que buscan causar daño a sus competidores y los recursos tecnológicos y humanos internos que puedan resultar dañinos para las organizaciones, sin olvidar todas aquellas amenazas emergentes y las acciones resultantes de la falta de cultura de ciberseguridad.

Por otra parte, la información digital se ha convertido en un activo de alto valor añadido. El análisis de los datos personales que circulan en la red se aprovecha para múltiples fines que abarca desde estudios sociológicos hasta campañas comerciales. El empleo malintencionado de datos personales y las campañas de desinformación tienen un alto potencial desestabilizador en la sociedad, y la explotación de brechas en los datos personales supone una violación a la seguridad de dichos datos, que afecta a la privacidad de las personas y a la integridad y confidencialidad de sus datos.

En cuanto a las campañas de desinformación, hacen uso de elementos como las noticias falsas para influir en la opinión pública. Internet y las redes sociales amplifican el efecto y alcance de la información transmitida, con potencial aplicación en contra de objetivos como por ejemplo organizaciones internacionales, Estados, iniciativas políticas o personajes públicos o incluso a procesos electorales democráticos.

## CAPÍTULO 3

## Propósito, principios y objetivos para la ciberseguridad

En este capítulo se establece el propósito y los principios por los que se rige la Estrategia, así como los objetivos: uno general y cinco específicos.

Propósito:

España precisa, tal y como establece la Estrategia de Seguridad Nacional de 2017, garantizar un uso seguro y responsable de las redes y los sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para un contribuir a la promoción de un ciberespacio seguro y fiable.

Por tanto, el propósito de la Estrategia Nacional de Ciberseguridad 2019, es fijar las directrices generales del ámbito de la ciberseguridad de manera que se alcancen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017.

Para ello, España ha de seguir avanzando en el refuerzo de capacidades para hacer frente a las ciberamenazas y el uso malicioso del ciberespacio. En consecuencia, se seguirán promoviendo medidas que ayuden a garantizar a nuestra nación su seguridad, con especial atención al sector público y los servicios esenciales, en un marco más coordinado y con estructuras de cooperación mejoradas.

Por otra parte, el fomento de la cultura de ciberseguridad ha de ser uno de los ejes centrales a desarrollar a fin de contar con una sociedad más conocedora de las amenazas y desafíos a las que se enfrenta. El derecho a hacer un uso seguro y fiable del ciberespacio y el contribuir a que así sea, es una responsabilidad compartida.

Asimismo, la ciberseguridad es progreso, por lo que el apoyo e impulso de la industria española de ciberseguridad, la promoción de un entorno que favorezca la investigación, el desarrollo y la innovación, y la participación del mundo académico tiene un carácter singular. Por otro lado, es un objetivo prioritario en nuestra sociedad alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas y profesionales, ya que solo mediante su promoción se podrá responder a los grandes retos de la ciberseguridad.

La transversalidad y globalidad del ciberespacio, requiere además de la cooperación y del cumplimiento del Derecho internacional, del máximo respeto a los principios recogidos en la Constitución y en la Carta de Naciones Unidas; en coherencia con la Estrategia de Seguridad Nacional y con las iniciativas desarrolladas en el marco europeo, regional e internacional, prevaleciendo en todo momento los intereses nacionales.

Principios rectores:

La Estrategia Nacional de Ciberseguridad, se sustenta y se inspira en los principios rectores de la Seguridad Nacional: unidad de acción, anticipación, eficiencia y resiliencia.

Unidad de Acción: Toda respuesta ante un incidente en el ámbito de la ciberseguridad que pueda implicar a distintos agentes del Estado se verá reforzada si es coherente, coordinada y se resuelve de manera rápida y eficaz, cualidades alcanzables a través de la adecuada preparación y articulación de la unidad de acción del Estado.

Una gestión centralizada de las crisis que afecten al ciberespacio, permite mantener una visión completa de la situación de la amenaza y posibilita el empleo de los recursos disponibles de forma más rápida, eficiente, coherente e integral.

Anticipación: La especificidad del ciberespacio y de los actores implicados demanda que existan mecanismos de anticipación en organismos especializados que orienten la Acción del Estado en situaciones de crisis, y en la que igualmente deber participar el sector privado.

La anticipación prima las actuaciones preventivas sobre las reactivas. Disponer de sistemas eficaces, con información compartida lo más próximo al tiempo real, permite alcanzar un adecuado conocimiento de la situación. Dicho factor resulta imprescindible para minimizar el tiempo de respuesta, lo que puede resultar crítico para reducir los efectos de las amenazas.

Eficiencia: La ciberseguridad precisa del empleo de sistemas multipropósito de gran valor y elevado nivel tecnológico, que llevan asociadas unas necesidades muy exigentes y un alto coste derivado de su desarrollo, adquisición y operación. A lo anterior se suma la necesidad de una planificación anticipada y una elevada complejidad en su sostenimiento.

Además, el escenario actual y futuro está marcado por la austeridad económica, que unida a la responsabilidad social de obtener el máximo rendimiento de los recursos disponibles, obliga a orientar la acción del Estado hacia la optimización y la eficiencia de los dedicados a la ciberseguridad, por lo que resultarán indispensables la unidad de acción, compartición de información e integración de estos recursos para alcanzar la eficiencia deseada.

Resiliencia: La resiliencia es una característica fundamental que deben poseer los sistemas e infraestructuras críticas. El Estado está obligado a asegurar la disponibilidad de los elementos que se consideren esenciales para la nación, mejorando su protección contra las ciberamenazas. Especial mención merece el refuerzo que requieren las redes de información y comunicaciones frente a actividades de las ciberamenazas o al uso ilícito del ciberespacio.

Objetivo general:

Los nuevos retos de la ciberseguridad han requerido la adaptación de su objetivo general de manera que se muestre más integrador, inclusivo y menos tecnificado.

En línea con la Estrategia de Seguridad Nacional de 2017 y ampliando el objetivo para la ciberseguridad previsto en la misma, España garantizará el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

Basados en este objetivo general, a continuación, se fijan una serie de objetivos específicos que orientan la acción del Estado en este ámbito.

*Objetivo I*

Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales

Es necesario consolidar un marco nacional coherente e integrado que ayude a garantizar la protección de la información manejada por el sector público y por los servicios esenciales, sus sistemas y servicios, así como de las redes que los soportan. Este marco permitirá desarrollar e implantar servicios cada vez más seguros y eficientes.

Para ello, es necesario implantar medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, desarrollando nuevas soluciones, reforzando la coordinación y adaptando en consecuencia el ordenamiento jurídico.

En particular, las acciones contra el ciberespionaje merecen especial mención para asegurar la protección del Patrimonio Tecnológico de España, entendido como aquellos activos materiales o inmateriales que sustentan la propiedad intelectual e industrial del sector empresarial, que conforman nuestro presente y condicionan el desarrollo futuro.

El sector público y los operadores de servicios esenciales se deben involucrar activamente en un proceso de mejora continua respecto de la protección de sus sistemas de Tecnologías de la Información y las Comunicaciones basados en una vigilancia permanente

de su exposición a las amenazas. Estos agentes deben servir como modelo de buenas prácticas en la gestión de la ciberseguridad.

En aplicación del principio de responsabilidad compartida, el sector público debe mantener estrechas relaciones con las empresas que gestionan los Sistemas de Tecnologías de la Información y las Comunicaciones relevantes para los intereses nacionales, intercambiando el conocimiento que permita una adecuada coordinación entre ambos y una cooperación efectiva que genere una sinergia apropiada dentro del entorno de la ciberseguridad.

El fortalecimiento de la ciberseguridad requiere un conocimiento sistemático sobre el impacto de una potencial interrupción o destrucción de las redes y sistemas que proporcionan servicios esenciales, así como métricas del nivel de seguridad de estos sistemas que permitan la oportuna toma de decisiones según su grado de exposición.

*Objetivo II*

Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso

El ciberespacio juega un papel cada vez más importante tanto en la comisión de hechos ilícitos o maliciosos como en su investigación para promover la confianza de los ciudadanos. Es necesario garantizar una adecuada persecución de los fenómenos criminales que en él se desarrollen.

Son tres los ámbitos en los que se desenvuelve la lucha contra la cibercriminalidad: (i) el ciberespacio como objetivo directo de los hechos delictivos, o de la amenaza; (ii) el ciberespacio como medio clave para su comisión; y (iii) el ciberespacio como medio u objeto directo de investigación de cualquier tipo de hecho ilícito.

Sobre la base de una regulación sólida y eficaz que refuerce y garantice la lucha contra la cibercriminalidad, es necesario el fortalecimiento de la cooperación judicial y policial, tanto nacional como internacional, así como la asignación de recursos suficientes a los órganos competentes en la materia y la capacitación de los profesionales que trabajan en este ámbito.

Del mismo modo, es fundamental fomentar la colaboración y participación ciudadana, facilitando los procedimientos de acceso y transmisión de la información de interés judicial y policial e identificando aspectos que requieran de una mejora en las capacidades de las instituciones policiales y de los organismos judiciales competentes.

*Objetivo III*

Protección del ecosistema empresarial y social y de los ciudadanos

Todas las personas y organizaciones tienen derecho a hacer un uso seguro del ciberespacio. Es por ello responsabilidad del Estado promover e impulsar las medidas para alcanzar y mantener un nivel suficiente de ciberseguridad, que proteja especialmente a los más vulnerables y que permita el adecuado desarrollo socioeconómico de España.

La ciberseguridad es una responsabilidad compartida con los actores privados que, por acción u omisión, puedan afectarla; y no es posible conseguirla sin su participación. Por tanto, entre las medidas a impulsar deben estar aquellas que conduzcan a la necesaria cooperación para la seguridad común.

La defensa de ciudadanos, autónomos y empresas debe ir más allá de las medidas de autoprotección que ellos puedan tomar, por lo que es conveniente implantar medidas para su ciberdefensa activa. A la vez todos los usuarios del ciberespacio deben hacer un uso responsable de la tecnología a su alcance.

La acelerada adopción por la sociedad de tecnologías emergentes provoca que los riesgos evolucionen. Por ello, el intercambio permanente de conocimiento con los diferentes actores y el establecimiento de mecanismos de monitorización para la protección del ecosistema empresarial y social serán instrumentos que permitirán al Gobierno estar informado y tomar las decisiones oportunas para actualizar y adecuar las acciones resultado de la presente estrategia.

*Objetivo IV*

Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas

Para afrontar los desafíos que plantea la ciberseguridad, España debe contar con recursos técnicos y humanos que le proporcionen la autonomía tecnológica necesaria y la capacitación adecuada para el uso seguro del ciberespacio, situando a la ciberseguridad como habilitador clave para una nación emprendedora.

Para ello, debe mejorar la ciberseguridad colectiva difundiendo la cultura de la ciberseguridad con la ayuda de organismos públicos y privados y medios de comunicación, potenciando mecanismos de información y asistencia a los ciudadanos y fomentando espacios de encuentro entre la sociedad civil, administraciones y empresas.

Se debe también contribuir al uso seguro y responsable de las Tecnologías de la Información y de las Comunicaciones promoviendo la capacitación en ciberseguridad de los profesionales adecuada a la demanda del mercado laboral, estimulando el desarrollo de los profesionales con habilidades propias, impulsando la formación y cualificación especializada, así como las capacidades de generación de conocimiento, el desarrollo actividades de I+D+i en ciberseguridad y el fomento del uso de productos y servicios certificados.

Asimismo, merece especial atención la protección del patrimonio tecnológico y de la propiedad industrial e intelectual. Para promover la soberanía tecnológica y aprovechar las oportunidades que ofrece la transformación digital, se fomentará e impulsará la industria española de ciberseguridad y las mejores prácticas en el desarrollo e implantación de sistemas de información y comunicaciones.

*Objetivo V*

Seguridad del ciberespacio en el ámbito internacional

España promoverá un ciberespacio abierto, plural, seguro y confiable tanto en sus relaciones bilaterales como en las organizaciones multilaterales, regionales e internacionales, y en los foros y conferencias, donde la ciberseguridad ocupa un lugar destacado.

Abogará por la creación de un marco internacional para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio, en el que se apliquen los principios de La Carta de Naciones Unidas en su totalidad, el Derecho Internacional, los Derechos Humanos y el Derecho Humanitario Bélico, así como las normas no vinculantes sobre el comportamiento responsable de los Estados.

Consciente de la importancia del multilateralismo, considera relevante el papel de Naciones Unidas para avanzar en la construcción de consensos que, junto a la adopción y puesta en marcha de medidas de fomento de la confianza, la colaboración y participación de todos los actores implicados (Estados, sector privado, sociedad civil, usuarios y academia), constituyen la base para lograr seguridad y estabilidad en el ciberespacio y avanzar hacia su regulación.

En línea con nuestros socios europeos, reforzará la confianza en Internet, en la transformación digital y en el desarrollo de las nuevas tecnologías, contribuyendo a consolidar un ecosistema cibernético europeo seguro que permita avances hacia el mercado único digital. Para ello defenderá un internet interoperativo, neutral, abierto y diverso, reflejo de la pluralidad cultural y lingüística internacional, basado en un sistema de gobernanza democrático, representativo e inclusivo, resultado de la concertación y el consenso. Además, un acceso a internet global y generalizado, contribuyendo con ello al cumplimiento de los Objetivos de Desarrollo Sostenible.

Del mismo modo, nuestra pertenencia a la Unión Europea (UE), nos obliga a fortalecer la seguridad y la autonomía estratégica europea mediante la búsqueda de sinergias, la cooperación técnica, operativa, estratégica y política; a reforzar nuestra resiliencia, nuestra capacidad de respuesta ante las crisis y las complementariedades entre los ámbitos civiles y militares como socios de la UE y aliados de la Organización del Tratado del Atlántico Norte (OTAN).

Sobre la base de lo anterior, España continuará participando activamente en la UE y la OTAN; en Naciones Unidas, y en sus foros derivados como el Foro de Gobernanza de Internet (IGF); en la Organización para la Seguridad y la Cooperación en Europa (OSCE), en el desarrollo e implementación de las Medidas de Fomento de la Confianza; en la Organización de Estados Americanos (OEA). Así como con el Foro Global del Expertos en Ciberseguridad (GFCE) y la Coalición por la Libertad en Internet (Freedom Online Coalition. FOC), sin olvidar nuestra presencia en el Centro Europeo de Excelencia para contrarrestar las Amenazas Híbridas (Hybrid CoE), así como en el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCD CoE).

Además, reforzará la cooperación internacional bilateral en materia de ciberseguridad, promoverá relaciones fluidas y de confianza en este ámbito, colaborará en la construcción de capacidades en terceros Estados, prestando especial atención a las mujeres y los jóvenes y fomentará la creación de canales de información e intercambio de experiencias, impulsando, para todo ello, la adopción de acuerdos bilaterales y multilaterales en este ámbito.

## CAPÍTULO 4

### Líneas de acción y medidas

En este capítulo se establecen las líneas de acción dirigidas a la consecución de los objetivos establecidos.

Línea de Acción 1. Reforzar las capacidades ante las amenazas provenientes del ciberespacio:

Esta línea de acción responde al Objetivo I de la Estrategia.

Medidas:

1. Ampliar y mejorar las capacidades de detección y análisis de las ciberamenazas de manera que se permita la identificación de procedimientos y orígenes de ataque, así como la elaboración de la inteligencia necesaria para una protección, atribución y defensa más eficaz.
2. Potenciar la colaboración de los centros de excelencia e investigación en la lucha contra las ciberamenazas.
3. Potenciar la creación, difusión y aplicación de mejores prácticas, y la adopción de estándares en materia de ciberseguridad.
4. Asegurar la coordinación técnica y operacional de los organismos con responsabilidades en ciberseguridad, las empresas y la sociedad.
5. Desarrollar y mantener actualizadas las normas, procedimientos e instrucciones de respuesta frente a incidentes de ciberseguridad, asegurando su integración en el Sistema de Seguridad Nacional.
6. Potenciar las capacidades de ciberdefensa y de ciberinteligencia.
7. Promover la participación de las empresas en plataformas sectoriales para el intercambio y análisis de información, así como para la medida del riesgo sectorial y la propuesta de acciones que lo mitiguen, acompañadas de requerimientos legales que las regulen.
8. Potenciar y apoyar los desarrollos realizados en la red de CSIRT española.
9. Impulsar el desarrollo de plataformas de notificación, intercambio de información y coordinación para la mejora de la ciberseguridad sectorial.
10. Desarrollar instrumentos de prevención, detección, respuesta, retorno a la normalidad y evaluación enfocados a la gestión de crisis para el ámbito de la ciberseguridad en el marco de la Seguridad Nacional.
11. Garantizar la coordinación, la cooperación y el intercambio de información sobre ciberincidentes e inteligencia de ciberamenazas entre el sector público, el sector privado y los organismos internacionales competentes, fomentando la prevención y la alerta temprana.
12. Implantar medidas de ciberdefensa activa en el sector público con el objetivo de mejorar las capacidades de respuesta.

Línea de Acción 2. Garantizar la seguridad y resiliencia de los activos estratégicos para España:

Esta línea de acción responde al Objetivo I de la Estrategia.
Medidas:

1. Ampliar y fortalecer las capacidades de prevención, detección, respuesta, recuperación y resiliencia a los ciberataques dirigidos al sector público, a los servicios esenciales y a empresas de interés estratégico.
2. Potenciar el desarrollo de la normativa sobre protección de infraestructuras críticas, reforzando la seguridad de las redes y sistemas de información que las soportan.
3. Asegurar la plena implantación del Esquema Nacional de Seguridad, del Sistema de Protección de las Infraestructuras Críticas, y el cumplimiento y armonización de la normativa sobre protección de infraestructuras críticas y servicios esenciales, con un enfoque prioritario basado en el riesgo.
4. Potenciar, en el marco de sus competencias, la progresiva implicación y creación de infraestructuras de ciberseguridad en las Comunidades Autónomas, las Ciudades Autónomas, las Entidades Locales y en sus organismos vinculados o dependientes que cooperarán y se coordinarán con las estructuras nacionales en pro de la mejora de la ciberseguridad nacional.
5. Desarrollar el Centro de Operaciones de Ciberseguridad de la Administración General del Estado que mejore las capacidades de prevención, detección y respuesta, e impulsar el desarrollo de centros de operaciones de ciberseguridad en el ámbito autonómico y local.
6. Reforzar la implantación de infraestructuras y servicios de telecomunicaciones y sistemas de información horizontales comunes, y compartidos por las Administraciones Públicas, potenciando su uso y sus capacidades de seguridad y resiliencia, asegurando a la par, la coordinación con los primeros en aquellos casos que no se utilicen las infraestructuras y servicios comunes.
7. Impulsar el desarrollo de un sistema de métricas de las principales variables de ciberseguridad que permita a las autoridades competentes determinar el nivel de seguridad y su evolución.
8. Comprometer al sector público y al privado en la gestión de los riesgos de la cadena de suministro, especialmente en aquellos que afecte a la provisión de servicios esenciales.
9. Desarrollar catálogos de productos y servicios cualificados y certificados, para su empleo en los procesos de contratación del sector público y de los servicios esenciales.
10. Reforzar las estructuras de seguridad y la capacidad de vigilancia de los sistemas de información que manejan información clasificada.
11. Promover la realización de ciberejercicios y evaluaciones de ciberseguridad, especialmente en áreas que puedan afectar a la Seguridad Nacional, la Administración pública, los servicios esenciales y las empresas cotizadas.
12. Asegurar la protección de las Infraestructuras Científico-Técnicas Singulares y los centros de referencia de I+D+i.

Línea de Acción 3. Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio:

Esta línea de acción responde al Objetivo II de la Estrategia.
Medidas:

1. Reforzar el marco jurídico para responder eficazmente a la cibercriminalidad, tanto en lo relativo a la definición de tipos penales como en la regulación de adecuadas medidas de investigación.
2. Fomentar la colaboración y participación ciudadana, articulando instrumentos de intercambio y transmisión de información de interés policial, y promoviendo el desarrollo de campañas de prevención de la cibercriminalidad orientadas a ciudadanos y empresas.
3. Reforzar las acciones encaminadas a potenciar las capacidades de investigación, atribución, persecución y, en su caso, la actuación penal, frente a la cibercriminalidad.
4. Fomentar el traslado a los organismos competentes de la jurisdicción penal de la información relativa a incidentes de seguridad que presenten caracteres de delito, y especialmente de aquellos que afecten o puedan afectar a la provisión de los servicios esenciales y a las infraestructuras críticas.

5. Procurar a los operadores jurídicos el acceso a información y recursos materiales que aseguren una mejor aplicación del marco jurídico y técnico relacionado con la lucha contra la cibercriminalidad, y que les dote de mayores capacidades para la investigación y enjuiciamiento de los hechos ilícitos que correspondan.

6. Fomentar el intercambio de información, experiencia y conocimientos, entre el personal con responsabilidades en la investigación y persecución de la cibercriminalidad.

7. Asegurar a los profesionales del Derecho y a las Fuerzas y Cuerpos de Seguridad del Estado el acceso a los recursos humanos y materiales que les proporcionen el nivel necesario de conocimientos para la mejor aplicación del marco legal y técnico asociado.

8. Impulsar la coordinación de las investigaciones sobre cibercriminalidad y otros usos ilícitos del ciberespacio entre los distintos órganos y unidades con competencia en esta materia.

9. Fortalecer la cooperación judicial y policial internacional.

Línea de Acción 4. Impulsar la ciberseguridad de ciudadanos y empresas:

Esta línea de acción responde al Objetivo III de la Estrategia.
Medidas:

1. Ofrecer a los ciudadanos y al sector privado un servicio público de ciberseguridad integrado, de calidad y de fácil acceso, y que sea un estímulo a la demanda de los servicios que ofrece el sector empresarial de la ciberseguridad.

2. Impulsar la ciberseguridad en las pymes, micropymes y autónomos mediante la articulación de políticas públicas en ciberseguridad, y especialmente con actuaciones dirigidas al fomento de la resiliencia.

3. Promover la ciberseguridad para garantizar la privacidad y protección de datos personales dentro del marco de los derechos digitales del ciudadano acorde con el ordenamiento jurídico, promoviendo la protección de la «identidad digital».

4. Crear mecanismos ágiles y seguros de denuncia para el sector privado y ciudadanos.

5. Estimular la cooperación entre actores públicos y privados, en particular promoviendo el compromiso de los Proveedores de Servicios de Internet y de Servicios Digitales para mejorar la ciberseguridad. Se impulsará la regulación nacional en este sentido y se implantarán medidas de ciberdefensa activa de ciudadanos y pymes.

6. Desarrollar mecanismos para la medida agregada del riesgo y su evolución, tanto de ciudadanos como de empresas, para priorizar medidas de ciberseguridad e informar adecuadamente a la sociedad.

7. Impulsar en el sector empresarial la implantación de estándares reconocidos de ciberseguridad. Estimular, junto con las entidades de normalización nacional e internacional, la creación, difusión y aplicación de mejores prácticas sectoriales en materia de ciberseguridad, incluidos diferentes esquemas de certificación.

8. Impulsar la implantación de sistemas fiables de identificación electrónica y servicios electrónicos de confianza.

9. Promover la creación del foro Nacional de Ciberseguridad, que integre a representantes de la sociedad civil, expertos independientes, sector privado, la academia, asociaciones, organismos sin ánimo de lucro, entre otros, con el objetivo de potenciar y crear sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

Línea de Acción 5. Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital:

Esta línea de acción responde al Objetivo IV de la Estrategia.
Medidas:

1. Impulsar programas de apoyo a la I+D+i en seguridad digital y ciberseguridad en pymes, empresas, universidades y centros de investigación, facilitando el acceso a programas de incentivos nacionales e internacionales y mediante programas de compra pública innovadora.

2. Dinamizar el sector industrial y de servicios de ciberseguridad, incentivando medidas de apoyo a la innovación, a la inversión, a la internacionalización y a la transferencia tecnológica en especial en el caso de micropymes y pymes.

3. Incrementar las actividades nacionales para el desarrollo de productos, servicios y sistemas de ciberseguridad, y la seguridad desde el diseño, apoyando específicamente aquellas que sustenten necesidades de interés nacional para fortalecer la autonomía digital, y la propiedad intelectual e industrial.

4. Promover las actividades de normalización y la exigencia de requisitos ciberseguridad en los productos y servicios de Tecnologías de la Información y de las Comunicaciones, facilitar el acceso a productos y servicios que respondan a estos requisitos, promoviendo la evaluación de la conformidad y la certificación, y apoyando la elaboración de catálogos.

5. Actualizar, o en su caso desarrollar marcos de competencias en ciberseguridad, que respondan a las necesidades del mercado laboral.

6. Identificar las necesidades de capacidades profesionales de ciberseguridad, fomentando la colaboración con las instituciones educativas y formativas impulsando la formación continua, la formación para el empleo y universitaria, promoviendo sistemas de acreditación y certificación profesional.

7. Impulsar la inclusión de perfiles profesionales de ciberseguridad en las relaciones de puestos de trabajo del sector público.

8. Detectar, fomentar y retener el talento en ciberseguridad, con especial atención al campo de la investigación.

9. Impulsar programas específicos de I+D+i en ciberseguridad y ciberdefensa.

Línea de Acción 6. Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales:

Esta línea de acción responde al Objetivo V de la Estrategia.

Medidas:

1. Potenciar y reforzar la presencia de España en las organizaciones, conferencias y foros regionales e internacionales y a los que pertenece y en los que la ciberseguridad forma parte sustancial de sus agendas, y apoyar y participar de manera activa en las diferentes iniciativas, coordinando la posición de los diferentes agentes nacionales implicados.

2. Promover en el ámbito de Naciones Unidas la búsqueda de consensos para el pleno respeto a la Carta de Naciones Unidas y la aplicación y puesta en práctica del Derecho Internacional y las normas para el comportamiento responsable de los Estados. Y del mismo modo avanzar en la adopción e implementación de Medidas para el Fomento de la Confianza en el ciberespacio.

3. Participar activamente en la Unión Europea en el desarrollo de un ecosistema europeo seguro que favorezca el avance y la consolidación del mercado único, y la seguridad y autonomía estratégica de Europa, buscando las complementariedades y la cooperación entre la Unión Europea y la OTAN.

4. Fomentar el diálogo bilateral, la cooperación y los sistemas de intercambio de información, alerta temprana y de experiencias para desarrollar un enfoque coordinado en la lucha contra las ciberamenazas con otros países, promoviendo la negociación y firma de acuerdos internacionales.

5. Promover el desarrollo de capacidades tecnológicas y el acceso a internet en terceros países para contribuir con ello al cumplimiento de los Objetivos de Desarrollo Sostenible.

6. Desarrollar con los países de nuestro entorno una mayor conciencia sobre las Amenazas Híbridas, limitando su impacto sobre la soberanía e integridad de nuestros países.

Línea de Acción 7. Desarrollar una cultura de ciberseguridad:

Las medidas incluidas en esta Línea de Acción contribuirán al Plan de Cultura de Seguridad Nacional y responde al objetivo IV de la Estrategia.

Medidas:

1. Incrementar las campañas de concienciación a ciudadanos y empresas, y poner a su disposición información útil adaptada a cada perfil, especialmente en el ámbito de los autónomos, pequeñas y medianas empresas.

2. Potenciar actuaciones encaminadas al incremento de la corresponsabilidad y obligaciones de la sociedad en la ciberseguridad nacional.

3. Impulsar iniciativas y planes de alfabetización digital en ciberseguridad.

4. Promover la difusión de la cultura de la ciberseguridad como una buena práctica empresarial, y reconocer la implicación de las empresas en la mejora de la ciberseguridad colectiva como responsabilidad social corporativa.

5. Promover un espíritu crítico en favor de una información veraz y de calidad y que contribuya a la identificación de las noticias falsas y la desinformación.

6. Concienciar a directivos de organizaciones, a los efectos de que habiliten los recursos necesarios y promuevan los proyectos de ciberseguridad que sus entidades puedan necesitar.

7. Promover la concienciación y formación en ciberseguridad en los centros de enseñanza, adaptada a todos los niveles formativos y especialidades.

8. Buscar y reconocer la colaboración y participación de medios de comunicación, para lograr un mayor alcance en las campañas dirigidas a ciudadanos y, en especial, a menores de edad.

## CAPÍTULO 5

### La ciberseguridad en el Sistema de Seguridad Nacional

En este capítulo se contempla la integración de la ciberseguridad en el actual Sistema de Seguridad Nacional.

La Estrategia de Ciberseguridad Nacional de 2013 y la posterior aprobación de la Ley de Seguridad Nacional de 2015 establecen una estructura orgánica específica para la ciberseguridad. En la presente Estrategia de 2019 se impulsan iniciativas que complementan los nuevos avances en el modelo de gobernanza nacional con las políticas europeas.

La estructura de la ciberseguridad en el marco del Sistema de Seguridad Nacional está constituida por los siguientes componentes:

1. El Consejo de Seguridad Nacional.
2. El Comité de Situación, único para el conjunto del Sistema de Seguridad Nacional ante situaciones de crisis.
3. El Consejo Nacional de Ciberseguridad.
4. La Comisión Permanente de Ciberseguridad.
5. El Foro Nacional de Ciberseguridad.
6. Las Autoridades públicas competentes y los CSIRT de referencia nacionales.

El Consejo de Seguridad Nacional:

El Consejo de Seguridad Nacional, en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, es el órgano al que corresponde asistir al Presidente del Gobierno en la dirección de la Política de Seguridad Nacional.

El Consejo de Seguridad Nacional actúa, a través del Departamento de Seguridad Nacional como punto de contacto único para ejercer una función de enlace y garantizar la cooperación transfronteriza con otros países de la Unión Europea.

El Comité de Situación:

El Comité de Situación tiene carácter único para el conjunto del Sistema de Seguridad Nacional y actuará, apoyado por el Departamento de Seguridad Nacional, de acuerdo con las directrices político-estratégicas dictadas por el Consejo de Seguridad Nacional en materia de gestión de crisis.

El Consejo Nacional de Ciberseguridad:

El Consejo Nacional de Ciberseguridad da apoyo al Consejo de Seguridad Nacional para el cumplimiento de sus funciones y, en particular, en la asistencia al Presidente del Gobierno en la dirección y coordinación de la Política de Seguridad Nacional en el ámbito de la ciberseguridad.

Entre sus funciones se encuentran reforzar las relaciones de coordinación, colaboración y cooperación entre las distintas Administraciones Públicas con competencias en materia de ciberseguridad, así como entre los sectores público y privado, y facilitar la toma de decisiones del propio Consejo mediante el análisis, estudio y propuesta de iniciativas tanto

en el ámbito nacional como en el internacional, así como realizar la valoración de los riesgos y amenazas, analizar los posibles escenarios de crisis, estudiar su posible evolución, elaborar y mantener actualizados los planes de respuesta y formular directrices para la realización de ejercicios de gestión de crisis en el ámbito de la ciberseguridad y evaluar los resultados de su ejecución, todo ello en coordinación con los órganos y autoridades directamente competentes.

La Comisión Permanente de Ciberseguridad:

La Comisión Permanente de Ciberseguridad se establece con objeto de facilitar la coordinación interministerial a nivel operacional en el ámbito de la ciberseguridad. Presidida por el Departamento de Seguridad Nacional, se compone de aquellos órganos y organismos representados en el Consejo Nacional de Ciberseguridad con responsabilidades operativas. Es el órgano al que corresponde asistir al Consejo Nacional de Ciberseguridad sobre aspectos relativos a la valoración técnica y operativa de los riesgos y amenazas a la ciberseguridad.

El funcionamiento de la Comisión se enmarca en el procedimiento de gestión de crisis en el ámbito de la ciberseguridad. Dicho procedimiento establece sus funciones dirigidas a detectar y valorar los riesgos y amenazas; facilitar el proceso de toma de decisiones y asegurar una respuesta óptima y coordinada de los recursos del Estado. Además, incluye los diferentes niveles de activación del Sistema de Seguridad Nacional, e instrucciones para la gestión de la comunicación pública.

A fin de responder de manera oportuna y proporcionada a situaciones de especial relevancia en el desarrollo de sus funciones, se progresará en la definición de sus capacidades y responsabilidades.

Foro Nacional de Ciberseguridad:

Actuará en la potenciación y creación de sinergias público privadas, particularmente en la generación de conocimiento sobre las oportunidades y los desafíos y amenazas a la seguridad en el ciberespacio.

La puesta en marcha del foro Nacional de Ciberseguridad, y la armonización de su funcionamiento con los órganos existentes, se realizará mediante la aprobación de las disposiciones normativas necesarias, con el objetivo de alcanzar el funcionamiento coordinado y eficiente de estos componentes en el Sistema de Seguridad Nacional.

Autoridades públicas competentes y los CSIRT de referencia nacionales:

El marco estratégico e institucional de la ciberseguridad se complementa con las autoridades públicas competentes en materia de seguridad de las redes y sistemas de información y los CSIRT de referencia nacional que se recogen en el marco jurídico nacional.

Asimismo, los CSIRT de las Comunidades Autónomas, de las Ciudades Autónomas, de las Entidades Locales y sus organismos vinculados o dependientes, los de las entidades privadas, la red de CSIRT.es y otros servicios de ciberseguridad relevantes deberán estar coordinados con los anteriores en función de las competencias de cada uno de ellos. De igual modo, desde los CSIRT nacionales, en colaboración con los CSIRT autonómicos y privados, se fomentará la puesta en marcha de iniciativas que contribuyan a la consecución de los objetivos de la estrategia nacional.

Consideraciones finales y evaluación:

La experiencia adquirida desde la Estrategia de Ciberseguridad Nacional de 2013, ha permitido plasmar en el presente documento una actualización de las amenazas y los desafíos a las que nos enfrentamos, siempre en continua evolución. Para adecuarse a este nuevo escenario cambiante, se proponen un conjunto de Líneas de Acción y medidas más dinámicas que permitan, si fuese necesario, una rápida adaptación del ecosistema de ciberseguridad nacional, basadas en un modelo de gobernanza con una considerable madurez, donde debe participar activamente el sector privado y el resto de la sociedad civil.

En este sentido, la Estrategia se concibe como un documento vivo que ha de adaptarse a la evolución de la ciberseguridad, por lo que deberá ser objeto de revisión continua, como también los planes específicos y sectoriales que de ella se deriven. Se elaborará un informe

anual de evaluación de la Estrategia donde figurará el grado de ejecución y cumplimiento de sus objetivos.

Por otro lado, a la vista del incremento de las amenazas y desafíos a la ciberseguridad y cómo los afrontan países de nuestro entorno, resulta cada vez más urgente dotarse de recursos económicos, humanos y materiales para hacer frente a los mismos. Una de las acciones especialmente relevantes en este marco es que el Centro de Operaciones de Ciberseguridad de la Administración General del Estado se encuentre adecuadamente dotado.

# § 53

## Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia

Jefatura del Estado
«BOE» núm. 134, de 5 de junio de 2013
Última modificación: 20 de diciembre de 2022
Referencia: BOE-A-2013-5940

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

### PREÁMBULO

#### I

El funcionamiento eficiente de los mercados y la existencia de una competencia efectiva son principios básicos de la economía de mercado, la cual impulsa y promueve la productividad de los factores y la competitividad general de la economía en beneficio de los consumidores. Estos principios son también fundamentales en el diseño y definición de las políticas regulatorias de las actividades económicas.

En este marco, los organismos supervisores tienen por objeto velar por el correcto funcionamiento de determinados sectores de la actividad económica, hacer propuestas sobre aspectos técnicos, así como resolver conflictos entre las empresas y la Administración.

La existencia de organismos independientes se justifica por la complejidad que, en determinados sectores caracterizados principalmente por la potencial existencia de fallos de mercado, tienen las tareas de regulación y supervisión, así como por la necesidad de contar con autoridades cuyos criterios de actuación se perciban por los operadores como eminentemente técnicos y ajenos a cualquier otro tipo de motivación.

El origen de los organismos reguladores independientes se remonta a 1887, cuando el Congreso de los Estados Unidos de América encomendó la regulación del sector ferroviario a una entidad independiente: la Comisión de Comercio Interestatal (ICC). Así comenzó un proceso que posteriormente se asentaría con la creación de la Federal Trade Comission en 1914 y con el impulso a las políticas antimonopolio. La experiencia americana de las llamadas comisiones reguladoras independientes se ha integrado en la forma típica de las actuaciones administrativas en los Estados Unidos que es la administración por agencias y ha obedecido a razones propias de su sistema jurídico y estructura administrativa que no se han planteado en los Derechos europeos.

En este lado del Atlántico, los países europeos corrigieron los fallos de funcionamiento de los mercados mediante la nacionalización de las empresas prestadoras de servicios públicos o la creación de sociedades públicas con esta finalidad. Por otro lado, las corrientes europeas de los años setenta del siglo pasado cristalizaron en fórmulas organizativas independientes a la búsqueda de una neutralidad y criterios de especialización técnica en sectores con presencia de intereses sociales muy relevantes, como el bursátil, el de la protección de datos informáticos o el audiovisual.

Confluyendo con las anteriores tendencias, no sería hasta los años ochenta y noventa cuando un amplio conjunto de países de la actual Unión Europea, incluido España, impulsado por las sucesivas directivas reguladoras de determinados sectores de red, tales como la energía, las telecomunicaciones o el transporte, llevó a cabo un intenso proceso liberalizador en el marco del mercado único, que trajo consigo reformas tendentes a asegurar la competencia efectiva en los mercados, la prestación de los servicios universales y la eliminación de las barreras de entrada y las restricciones sobre los precios.

En este contexto surgió un amplio debate sobre el grado en que los nuevos mercados que se abrían a la competencia debían estar sometidos a las normas y autoridades de defensa de la competencia nacionales o si, por el contrario, debían ser los nuevos organismos sectoriales independientes los que llevaran a cabo la supervisión.

En el caso de España, se optó por una separación de funciones. Las autoridades sectoriales se encargaron de asegurar la separación vertical de las empresas entre los sectores regulados y sectores en competencia y resolver los conflictos que pudieran surgir entre los diferentes operadores, especialmente en los casos en que era necesario garantizar el libre acceso a infraestructuras esenciales. Junto a ello, se atribuyeron a los nuevos organismos potestades de inspección y sanción, así como distintas funciones de proposición normativa económica y técnica y la elaboración de estudios y trabajos sobre el sector.

Por su parte, la Autoridad de Defensa de la Competencia ha venido ejerciendo lo que se denomina un control ex post de la libre competencia, investigando y sancionando las conductas contrarias a la normativa de defensa de la competencia, y un control ex ante, examinando las operaciones de concentración empresarial.

Transcurrido cierto tiempo desde la implantación de este sistema, que ha reportado indudables ventajas para el proceso de liberalización y transición a la competencia de los sectores regulados, es necesario revisarlo.

Desde 2011 ha crecido notablemente el número de estos organismos. Hasta entonces eran cinco: Comisión Nacional de Energía, Comisión del Mercado de las Telecomunicaciones, Comisión Nacional de la Competencia, Comité de Regulación Ferroviaria y Comisión Nacional del Sector Postal. La Ley 2/2011, de 4 de marzo, de Economía Sostenible, previó la constitución de un sexto, el organismo regulador del sector del transporte. Más tarde, se aprobó la creación de la Comisión Nacional del Juego y la Comisión de Regulación Económica Aeroportuaria. A ellos hay que unir el Consejo Estatal de Medios Audiovisuales, regulado en la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual.

A la hora de plantear la revisión del sistema, el primer elemento que ha de tomarse en consideración es algo que debe caracterizar, no ya a cualquier mercado, sino a todos los sectores de la actividad económica: la seguridad jurídica y la confianza institucional. Estas se consiguen con unas normas claras, una arquitectura institucional seria y unos criterios de actuación conocidos y predecibles por todos los agentes económicos. Cuanto mayor sea la proliferación de organismos con facultades de supervisión sobre la misma actividad, más intenso será el riesgo de encontrar duplicidades innecesarias en el control de cada operador y decisiones contradictorias en la misma materia.

En segundo lugar, de modo especialmente importante en el entorno de austeridad en el que se encuentra la Administración Pública, se deben aprovechar las economías de escala derivadas de la existencia de funciones de supervisión idénticas o semejantes, metodologías y procedimientos de actuación similares y, sobre todo, conocimientos y experiencia cuya utilización en común resulta obligada.

En tercer lugar, las instituciones han de adaptarse a la transformación que tiene lugar en los sectores administrados. Debe darse una respuesta institucional al progreso tecnológico, de modo que se evite el mantenimiento de autoridades estancas que regulan ciertos

aspectos de sectores que, por haber sido objeto de profundos cambios tecnológicos o económicos, deberían regularse o supervisarse adoptando una visión integrada.

En los últimos años, se detecta una clara tendencia a nivel internacional a fusionar autoridades relacionadas con un único sector o con sectores que presentan una estrecha relación, pasando del modelo uni-sectorial a un modelo de convergencia orgánica, material o funcional en actividades similares o a un modelo multisectorial para sectores con industrias de red. Las ventajas que han motivado la adopción de estos modelos son las de optimizar las economías de escala y garantizar el enfoque consistente de la regulación en todas las industrias de red. Además, se ha argumentado que el riesgo de captura del regulador, tanto por el sector privado como por el gobierno, es menor en el caso de las autoridades multisectoriales, al reducirse la importancia relativa de un determinado sector o de un determinado ministerio para la autoridad.

Por último, en algunos casos, como el de los Países Bajos, se han integrado las autoridades reguladoras de ciertos sectores en la autoridad de competencia. Con ello se consigue una mayor eficacia en la supervisión de la competencia en los mercados, al poder contar de forma inmediata con el conocimiento de los reguladores sectoriales, que ejercen un control continuo sobre sus respectivos sectores a través de instrumentos de procesamiento de datos más potentes.

La situación actual en España, en la que se ha aprobado la creación de ocho organismos supervisores vinculados a los mercados de productos y de servicios y se ha previsto la creación de otro más, debe evolucionar hacia los modelos que se están implantando en los países de nuestro entorno. La filosofía que subyace en la existencia de todos estos organismos es fundamentalmente velar por unos mercados competitivos y unos servicios de calidad, en beneficio de los ciudadanos. La presencia de todas estas entidades de forma separada, con sus respectivos órganos de gobierno y medios materiales, exige una reforma de calado teniendo en cuenta la existencia de funciones, procedimientos, metodologías y conocimientos que, por su identidad o semejanza, bien podrían ejercerse o aplicarse por una sola institución.

La normativa europea prevé la existencia de autoridades reguladoras nacionales independientes, dotándolas de misiones, objetivos y competencias concretas. No obstante, las competencias de las comisiones en España son más amplias que las requeridas por la normativa europea, en lo referente a la política sectorial, la concesión y revocación de títulos habilitantes para el ejercicio de determinadas actividades, el asesoramiento al Gobierno y el estudio e investigación de los sectores.

Por ello, el objeto de esta Ley es la creación de la Comisión Nacional de los Mercados y la Competencia, que agrupará las funciones relativas al correcto funcionamiento de los mercados y sectores supervisados por la Comisión Nacional de Energía, la Comisión del Mercado de las Telecomunicaciones, la Comisión Nacional de la Competencia, el Comité de Regulación Ferroviaria, la Comisión Nacional del Sector Postal, la Comisión de Regulación Económica Aeroportuaria y el Consejo Estatal de Medios Audiovisuales.

II

La Ley consta de treinta y nueve artículos agrupados en cinco capítulos, dieciocho disposiciones adicionales, diez disposiciones transitorias, una disposición derogatoria, once disposiciones finales y un anexo.

El Capítulo I, «Naturaleza y régimen jurídico», procede a la creación de la Comisión Nacional de los Mercados y la Competencia, cuyo objeto es garantizar, preservar y promover el correcto funcionamiento del mercado, así como la transparencia y la existencia de una competencia efectiva en todos los mercados y sectores productivos en beneficio de los consumidores y usuarios. La Comisión se configura como un organismo público de los previstos en la Disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

La Comisión está dotada de personalidad jurídica propia y plena capacidad pública y privada y actuará con pleno sometimiento a la ley, con autonomía orgánica y funcional y con plena independencia del Gobierno, de las Administraciones Públicas y de cualquier interés empresarial y comercial. Sin perjuicio de su independencia, la Comisión velará por la aplicación uniforme de la normativa sectorial y general de competencia en el territorio

nacional mediante la cooperación con la Administración General del Estado, con las Comunidades Autónomas, con los órganos jurisdiccionales, con las instituciones y organismos de la Unión Europea, en especial con la Comisión Europea, y con las autoridades competentes y organismos de otros Estados miembros en el desarrollo de su actividad.

El Capítulo II, «Funciones», expone las funciones de la Comisión Nacional de los Mercados y la Competencia. Dichas funciones pueden clasificarse en dos grandes grupos. Por un lado, la Comisión ejercerá funciones, con carácter general, en el conjunto de mercados para la defensa y promoción de la competencia en los mismos. Estas funciones son tanto de supervisión como de arbitraje y consultivas.

Es de destacar que las funciones de defensa de la competencia recogidas en la Ley 15/2007, de 3 de julio, de Defensa de la Competencia, se atribuyen íntegramente a la Comisión Nacional de los Mercados y la Competencia. Esta reforma no afecta al contenido sustantivo de la Ley 15/2007, de 3 de julio, que permanece igual salvo en el esquema institucional de aplicación de la norma.

Por otro lado, la Comisión ejercerá funciones, con carácter singular, en determinados sectores y mercados regulados, donde la aplicación de la normativa de defensa de la competencia resulta insuficiente para garantizar la existencia de una competencia efectiva. Estos sectores o ámbitos son los siguientes: las comunicaciones electrónicas y la comunicación audiovisual, los mercados de la electricidad y de gas natural, el sector postal, las tarifas aeroportuarias y determinados aspectos del sector ferroviario.

Las funciones que la Comisión ejercerá sobre los citados sectores han sido tradicionalmente desempeñadas por los organismos reguladores sectoriales, por requerirse la independencia respecto de los intereses públicos que pudiesen confluir. En particular, abarcan funciones de supervisión y control, así como funciones de resolución de conflictos, más amplias y flexibles que las de mero arbitraje.

Respecto de las funciones a desarrollar por el nuevo organismo, cabe señalar que se ha procedido a una reordenación de funciones entre la Comisión Nacional de los Mercados y la Competencia y los departamentos ministeriales correspondientes. Las disposiciones adicionales sexta a undécima aclaran qué funciones concretas asumirá cada Ministerio. Con esta reestructuración funcional, la Ley persigue ante todo la eficacia de la intervención pública. En general, los Ministerios pasan a asumir todas aquellas tareas de índole administrativa que venían ejerciendo los organismos reguladores, para cuyo desempeño no se requiere una especial independencia, así como tareas que resultaban de escasa utilidad para la consecución de los objetivos de la Comisión. Ello permite que la nueva Comisión Nacional de los Mercados y la Competencia concentre su actuación en las funciones que verdaderamente sirven a su objeto fundamental, velar por un funcionamiento correcto de los mercados y la libre concurrencia.

El Capítulo III, «Organización y funcionamiento», regula la composición, el régimen de nombramiento y cese y las funciones de los órganos rectores de la Comisión, que comprenden el Consejo y el Presidente de la Comisión.

El Consejo se configura como el órgano colegiado de decisión de la Comisión y entre sus funciones se encuentran las de resolver y dictaminar los asuntos que la Comisión tiene atribuidos y la de resolver los procedimientos sancionadores. El Consejo actúa en pleno y en salas, una dedicada a temas de competencia y otra a temas de supervisión regulatoria.

El Consejo se compone de diez miembros: un Presidente, un Vicepresidente y ocho consejeros. Todos los miembros del Consejo, incluidos el Presidente y el Vicepresidente, son nombrados por el Gobierno mediante Real Decreto, pudiendo el Congreso vetar el nombramiento del candidato propuesto. Con la introducción de esta nueva exigencia de aceptación por parte del Congreso se refuerza la legitimidad democrática de la Comisión. El mandato de los miembros del Consejo será de seis años sin posibilidad de reelección.

Por otro lado, se regula la estructura básica de los órganos de dirección, estableciéndose cuatro direcciones de instrucción, una para la instrucción de los expedientes de defensa de la competencia y otras tres para la instrucción de los asuntos de supervisión regulatoria en los sectores de las telecomunicaciones y servicios audiovisuales, de la energía y, por último, de los transportes y del sector postal.

Debe subrayarse la atribución a la Dirección de Competencia de todas las funciones de instrucción recogidas en la Ley 15/2007, de 3 de julio, que, como actualmente, seguirán ejerciéndose manteniendo la unicidad, coherencia y el carácter horizontal de la normativa de defensa de la competencia.

Finalmente, se sientan las bases legales del régimen de funcionamiento de la Comisión, que serán desarrolladas por el Gobierno mediante Real Decreto, con la aprobación del Estatuto Orgánico de la Comisión Nacional de los Mercados y la Competencia, y por el propio Consejo de la Comisión, a través del Reglamento de funcionamiento interno. El Estatuto determinará la estructura interna de las Direcciones y demás áreas de responsabilidad, garantizando la debida separación entre las funciones de instrucción y resolución.

El Capítulo IV, «Régimen de actuación y potestades», regula los aspectos esenciales en relación a las facultades de inspección y supervisión, a la potestad sancionadora, al régimen de contratación y del personal y al régimen económico-financiero, patrimonial y presupuestario. Por último, para garantizar la independencia de las decisiones de la Comisión, se prevé que las resoluciones adoptadas por el Consejo, tanto en pleno como en salas, pongan fin a la vía administrativa, siendo impugnables únicamente ante la jurisdicción contencioso-administrativa.

El Capítulo V, «Transparencia y responsabilidad», delimita todos aquellos asuntos que la Comisión deberá hacer públicos y regula el control que el Congreso y el Senado ejercerán sobre la Comisión. Lo regulado en este Capítulo se inspira en gran medida en las novedades introducidas en la materia por la Ley 2/2011, de 4 de marzo, de Economía Sostenible.

La transparencia de la actuación de la Comisión es un elemento que refuerza su legitimidad y contribuye a infundir la necesaria confianza de los ciudadanos en la institución. En este sentido, se requiere a la Comisión que haga públicos todos aquellos informes que emita, la memoria anual de actividades y los planes anuales o plurianuales. La Comisión también deberá hacer públicos los acuerdos y resoluciones adoptados por el Consejo y la organización y funciones de cada uno de sus órganos y dispondrá de un órgano de control interno. El control parlamentario se efectúa a través de las comparecencias del Presidente ante el Congreso, que tendrán como mínimo una periodicidad anual.

Las disposiciones adicionales regulan una serie de aspectos complementarios destinados a permitir la reforma institucional introducida por esta Ley. Se prevé la constitución de la Comisión Nacional de los Mercados y la Competencia en el plazo máximo de cuatro meses desde la entrada en vigor de la Ley; la extinción de los organismos cuyas funciones se asumen por la Comisión; la integración de los bienes sobrantes de la fusión en el patrimonio de la Administración General del Estado; las funciones que asumen los distintos departamentos ministeriales en relación a los mercados regulados; y la integración del personal de los organismos que se extinguen en la Comisión Nacional de los Mercados y la Competencia o en la Administración General del Estado, según proceda.

Por su parte, las disposiciones transitorias regulan determinados aspectos necesarios para la puesta en marcha del nuevo organismo, relativos al primer mandato de los consejeros; al desempeño de funciones por los organismos reguladores que se extinguirán mientras la nueva Comisión no se ponga en funcionamiento; a la continuación de los expedientes pendientes por la Comisión o el Ministerio competente, según proceda; a los presupuestos de la Comisión y al régimen de personal.

Las disposiciones derogatoria y finales efectúan las derogaciones y modificaciones de las normas con rango de ley que resultan afectadas por la entrada en vigor de esta norma, prevén el desarrollo reglamentario, la habilitación competencial y la entrada en vigor de la Ley.

El Anexo incluye las tasas y prestaciones patrimoniales de carácter público relacionadas con las actividades y servicios regulados en la Ley, cuyo ingreso se efectuará en el Tesoro Público.

CAPÍTULO I

**Naturaleza y régimen jurídico**

**Artículo 1.** *La Comisión Nacional de los Mercados y la Competencia.*

1. Se crea la Comisión Nacional de los Mercados y la Competencia, como organismo público de los previstos en la Disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

2. La Comisión Nacional de los Mercados y la Competencia tiene por objeto garantizar, preservar y promover el correcto funcionamiento, la transparencia y la existencia de una competencia efectiva en todos los mercados y sectores productivos, en beneficio de los consumidores y usuarios.

3. A los efectos de lo establecido en el apartado anterior, la Comisión Nacional de los Mercados y la Competencia ejercerá sus funciones en todo el territorio español y en relación con todos los mercados o sectores económicos.

**Artículo 2.** *Naturaleza y régimen jurídico.*

1. La Comisión Nacional de los Mercados y la Competencia está dotada de personalidad jurídica propia y plena capacidad pública y privada y actúa, en el desarrollo de su actividad y para el cumplimiento de sus fines, con autonomía orgánica y funcional y plena independencia del Gobierno, de las Administraciones Públicas y de los agentes del mercado. Asimismo, está sometida al control parlamentario y judicial.

2. La Comisión Nacional de los Mercados y la Competencia se regirá por lo dispuesto en esta Ley, en la Ley 15/2007, de 3 de julio, de Defensa de la Competencia, y en la legislación especial de los mercados y sectores sometidos a su supervisión a que hacen referencia los artículos 6 a 11 de esta Ley y, supletoriamente, por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, por la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, de acuerdo con lo previsto en su Disposición adicional décima, por la Ley 47/2003, de 26 de noviembre, General Presupuestaria, y por el resto del ordenamiento jurídico.

3. La Comisión Nacional de los Mercados y la Competencia tendrá su sede principal en Madrid. El Real Decreto por el que se apruebe su Estatuto Orgánico podrá prever la existencia de otras sedes.

4. La Comisión Nacional de los Mercados y la Competencia está adscrita al Ministerio de Economía y Competitividad, sin perjuicio de su relación con los Ministerios competentes por razón de la materia en el ejercicio de las funciones a que se refieren los artículos 5 a 12 de esta Ley.

**Artículo 3.** *Independencia funcional y relación con las entidades públicas y privadas.*

1. La Comisión Nacional de los Mercados y la Competencia actuará, en el desarrollo de su actividad y para el cumplimiento de sus fines, con independencia de cualquier interés empresarial o comercial.

2. En el desempeño de las funciones que le asigna la legislación, y sin perjuicio de la colaboración con otros órganos y de las facultades de dirección de la política general del Gobierno ejercidas a través de su capacidad normativa, ni el personal ni los miembros de los órganos de la Comisión Nacional de los Mercados y la Competencia podrán solicitar o aceptar instrucciones de ninguna entidad pública o privada.

**Artículo 4.** *Coordinación y cooperación institucional.*

1. La Comisión Nacional de los Mercados y la Competencia velará por la aplicación uniforme de la normativa sectorial y general de competencia en todo el territorio mediante la coordinación con los órganos competentes de las Comunidades Autónomas y la cooperación con la Administración General del Estado y con los órganos jurisdiccionales.

2. Asimismo, la Comisión Nacional de los Mercados y la Competencia mantendrá una colaboración regular y periódica con las instituciones y organismos de la Unión Europea, en

especial, con la Comisión Europea y con las autoridades competentes y organismos de otros Estados miembros, fomentando la coordinación de las actuaciones respectivas en los términos previstos en la legislación aplicable. En particular, fomentará la colaboración y cooperación con la Agencia de Cooperación de los Reguladores de la Energía y con el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas.

## CAPÍTULO II

## Funciones

**Artículo 5.** *Funciones de la Comisión Nacional de los Mercados y la Competencia de carácter general y para preservar y promover la competencia efectiva en todos los mercados y sectores productivos.*

1. Para garantizar, preservar y promover el correcto funcionamiento, la transparencia y la existencia de una competencia efectiva en todos los mercados y sectores productivos, en beneficio de los consumidores y usuarios, la Comisión Nacional de los Mercados y la Competencia realizará las siguientes funciones:

a) Supervisión y control de todos los mercados y sectores económicos.

b) Realizar las funciones de arbitraje, tanto de derecho como de equidad, que le sean sometidas por los operadores económicos en aplicación de la Ley 60/2003, de 23 de diciembre, de Arbitraje, así como aquellas que le encomienden las leyes, sin perjuicio de las competencias que correspondan a los órganos competentes de las Comunidades Autónomas en sus ámbitos respectivos.

El ejercicio de esta función arbitral no tendrá carácter público. El procedimiento arbitral se regulará mediante Real Decreto y se ajustará a los principios esenciales de audiencia, libertad de prueba, contradicción e igualdad.

c) Aplicar lo dispuesto en la Ley 15/2007, de 3 de julio, en materia de conductas que supongan impedir, restringir y falsear la competencia, sin perjuicio de las competencias que correspondan a los órganos autonómicos de defensa de la competencia en su ámbito respectivo y de las propias de la jurisdicción competente.

d) Aplicar lo dispuesto en la Ley 15/2007, de 3 de julio, en materia de control de concentraciones económicas.

e) Aplicar lo dispuesto en la Ley 15/2007, de 3 de julio, en materia de ayudas públicas.

f) Aplicar en España los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea y su Derecho derivado, sin perjuicio de las competencias que correspondan en el ámbito de la jurisdicción competente.

g) Adoptar medidas y decisiones para aplicar los mecanismos de cooperación, asistencia mutua y asignación de expedientes con la Comisión Europea y otras Autoridades Nacionales de Competencia de los Estados miembros previstos en la normativa europea y, en particular, en el Reglamento (CE) n.º 1/2003 del Consejo, de 16 de diciembre de 2002, relativo a la aplicación de las normas sobre competencia previstas en los artículos 81 y 82 del Tratado de la Comunidad Europea (actuales artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea), en el Reglamento (CE) n.º 139/2004 del Consejo, de 20 de enero de 2004, sobre el control de las concentraciones entre empresas y sus normas de desarrollo y en la Directiva (UE) 2019/1 del Parlamento Europeo y del Consejo de 11 de diciembre de 2018, encaminada a dotar a las autoridades de competencia de los Estados miembros de medios para aplicar más eficazmente las normas sobre competencia y garantizar el correcto funcionamiento del mercado interior.

h) Promover y realizar estudios y trabajos de investigación en materia de competencia, así como informes generales sobre sectores económicos.

i) Realizar cualesquiera otras funciones que le sean atribuidas por Ley o por Real Decreto.

2. La Comisión Nacional de los Mercados y la Competencia actuará como órgano consultivo sobre cuestiones relativas al mantenimiento de la competencia efectiva y buen funcionamiento de los mercados y sectores económicos. En particular, podrá ser consultada por las Cámaras Legislativas, el Gobierno, los departamentos ministeriales, las

Comunidades Autónomas, las Corporaciones locales, los Colegios Profesionales, las Cámaras de Comercio y las Organizaciones Empresariales y de Consumidores y Usuarios. En ejercicio de esta función, llevará a cabo las siguientes actuaciones:

a) Participar, mediante informe, en el proceso de elaboración de normas que afecten a su ámbito de competencias en los sectores sometidos a su supervisión, a la normativa de defensa de la competencia y a su régimen jurídico.

b) Informar sobre los criterios para la cuantificación de las indemnizaciones que los autores de las conductas previstas en los artículos 1, 2 y 3 de la Ley 15/2007, de 3 de julio, deban satisfacer a los denunciantes y a terceros que hubiesen resultado perjudicados como consecuencia de aquéllas, cuando le sea requerido por el órgano judicial competente.

c) Informar sobre todas las cuestiones a que se refiere el artículo 16 de la Ley 15/2007, de 3 de julio, y el Reglamento (CE) n.º 1/2003 del Consejo, de 16 de diciembre de 2002, relativo a la aplicación de las normas sobre competencia previstas en los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea en cuanto a los mecanismos de cooperación con los órganos jurisdiccionales nacionales.

d) Cualesquiera otras cuestiones sobre las que deba informar, de acuerdo con lo previsto en la normativa vigente.

3. Sin perjuicio de lo dispuesto en los apartados 1 y 2, en los mercados de comunicaciones electrónicas y comunicación audiovisual, en el sector eléctrico y en el sector de gas natural, en el sector ferroviario, en materia de tarifas aeroportuarias y el mercado postal, la Comisión Nacional de los Mercados y la Competencia estará a lo dispuesto en los artículos 6 a 11 de esta Ley.

4. En cumplimiento de sus funciones, la Comisión Nacional de los Mercados y la Competencia está legitimada para impugnar ante la jurisdicción competente los actos de las Administraciones Públicas sujetos al Derecho administrativo y disposiciones generales de rango inferior a la ley de los que se deriven obstáculos al mantenimiento de una competencia efectiva en los mercados.

5. Para el ejercicio de sus funciones, la Comisión Nacional de los Mercados y la Competencia dispondrá, de conformidad con lo establecido por el Capítulo IV de esta Ley en materia presupuestaria, de recursos financieros y humanos adecuados, incluidos los necesarios para participar activamente en las actividades de la Agencia de Cooperación de los Reguladores de la Energía y del Organismo de Reguladores Europeos de las Comunicaciones Electrónicas y contribuir a las mismas.

**Artículo 6.** *Supervisión y control del mercado de comunicaciones electrónicas.*

La Comisión Nacional de los Mercados y la Competencia supervisará y controlará el correcto funcionamiento de los mercados de comunicaciones electrónicas. En particular, ejercerá las siguientes funciones:

1. Definir y analizar los mercados de referencia relativos a redes y servicios de comunicaciones electrónicas, entre los que se incluirán los correspondientes mercados de referencia al por mayor y al por menor, y el ámbito geográfico de los mismos, cuyas características pueden justificar la imposición de obligaciones específicas, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y su normativa de desarrollo.

2. Identificar el operador u operadores que poseen un poder significativo en el mercado cuando del análisis de los mercados de referencia se constate que no se desarrollan en un entorno de competencia efectiva.

3. Establecer, cuando proceda, las obligaciones específicas que correspondan a los operadores con poder significativo en mercados de referencia, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, y su normativa de desarrollo.

4. Resolver los conflictos en los mercados de comunicaciones electrónicas a los que se refiere el artículo 12.1.a) de la presente Ley.

5. Realizar las funciones atribuidas por la Ley 32/2003, de 3 de noviembre, y su normativa de desarrollo.

6. Realizar cualesquiera otras funciones que le sean atribuidas por Ley o por Real Decreto.

**Artículo 7.** *Supervisión y control en el sector eléctrico y en el sector del gas natural.*

La Comisión Nacional de los Mercados y la Competencia ejercerá las siguientes funciones en el ámbito del sector eléctrico y del sector del gas natural:

1. Establecer, mediante circulares dictadas de conformidad con el artículo 30 de esta ley, previo trámite de audiencia y con criterios de eficiencia económica, transparencia, objetividad y no discriminación, y de acuerdo con las orientaciones de política energética:

a) La estructura y la metodología para el cálculo de los peajes de acceso a las redes de electricidad destinados a cubrir la retribución del transporte y la distribución. La estructura y metodología deberán respetar las orientaciones de política energética y, en particular, el principio de sostenibilidad económica y financiera del sistema eléctrico de conformidad con la Ley 24/2013, de 26 de diciembre.

b) La metodología relativa al acceso a las infraestructuras transfronterizas, incluidos los procedimientos para asignar capacidad y gestionar la congestión en los sectores de electricidad y gas.

c) Las metodologías relativas a la prestación de servicios de balance y de no frecuencia del sistema eléctrico que, desde el punto de vista de menor coste, de manera justa y no discriminatoria proporcionen incentivos adecuados para que los usuarios de la red equilibren su producción y consumo.

d) La estructura y la metodología para el cálculo de los peajes y cánones de los servicios básicos de acceso a las instalaciones gasistas destinados a cubrir la retribución asociada al uso de las instalaciones de las redes de transporte, distribución y plantas de gas natural licuado. La estructura y la metodología deberán respetar las orientaciones de política energética y, en particular, el principio de sostenibilidad económica y financiera del sistema gasista de conformidad con la Ley 18/2014, de 15 de octubre.

e) La metodología relativa a la prestación de servicios de balance de forma que proporcionen incentivos adecuados para que los usuarios de la red equilibren sus entradas y salidas del sistema gasista. Los servicios de balance se facilitarán de manera justa y no discriminatoria y se basarán en criterios objetivos dentro del marco normativo de acceso y funcionamiento del sistema establecido en la Ley 34/1998, de 7 de octubre.

f) Las metodologías utilizadas para calcular las condiciones para la conexión y acceso a las redes de gas y electricidad.

g) La metodología, los parámetros y la base de activos para la retribución de las instalaciones de transporte y distribución de energía eléctrica conforme las orientaciones de política energética.

Entre otros, corresponderá a la Comisión Nacional de los Mercados y la Competencia fijar, en su caso, los valores unitarios de inversión, de operación y mantenimiento y la vida útil regulatoria de las instalaciones con derecho a retribución a cargo del sistema eléctrico de las empresas de transporte y distribución para cada periodo regulatorio.

Asimismo, le corresponderá a la Comisión Nacional de los Mercados y la Competencia fijar la tasa de retribución financiera de las instalaciones con derecho a retribución a cargo del sistema eléctrico de las empresas de transporte y distribución para cada periodo regulatorio. Esta tasa no podrá exceder de lo que resulte de conformidad con lo establecido en la Ley 24/2013, de 26 de diciembre y demás normativa de aplicación.

Excepcionalmente, el referido valor podrá superarse por la Comisión Nacional de los Mercados y la Competencia, de forma motivada y previo informe del Ministerio para la Transición Ecológica, en casos debidamente justificados. En este supuesto, la Comisión hará constar el impacto de su propuesta en términos de costes para el sistema respecto del que se derivaría de aplicar el valor anteriormente resultante.

h) La metodología, los parámetros y la base de activos para la retribución de las instalaciones de transporte y distribución de gas natural y plantas de gas natural licuado, conforme orientaciones de política energética.

Entre otros, corresponderá a la Comisión Nacional de los Mercados y la Competencia fijar, en su caso, los valores unitarios de inversión, de operación y mantenimiento y la vida útil regulatoria de los activos con derecho a retribución a cargo del sistema de gas natural de las empresas de distribución, transporte y plantas de gas natural licuado para cada periodo regulatorio.

Asimismo, le corresponderá a la Comisión Nacional de los Mercados y la Competencia fijar la tasa de retribución financiera de los activos de transporte, distribución y plantas de gas natural licuado con derecho a retribución a cargo del sistema gasista para cada periodo regulatorio. Esta tasa no podrá exceder de la que resulte de conformidad con lo establecido en la ley 18/2014, de 15 de octubre y demás normativa de aplicación.

Excepcionalmente, el referido valor podrá superarse por la Comisión Nacional de los Mercados y la Competencia, de forma motivada y previo informe del Ministerio para la Transición Ecológica, en casos debidamente justificados. En este supuesto, la Comisión hará constar el impacto de su propuesta en términos de costes para el sistema respecto del que se derivaría de aplicar el valor anteriormente resultante.

i) La metodología para el cálculo de la retribución del operador del sistema eléctrico y del gestor técnico del sistema gasista, en función de los servicios que efectivamente presten. Dichas retribuciones podrán incorporar incentivos, que podrán tener signos positivos o negativos, a la reducción de costes de los sistemas eléctricos y gasistas derivados de la operación de los mismos u otros objetivos.

Las Circulares anteriormente mencionadas, así como los actos de ejecución y aplicación de las mismas, serán publicados en el “Boletín Oficial del Estado”.

1 bis. Aprobar, mediante resolución, los valores de los peajes de acceso a las redes de electricidad y gas, así como las cuantías de la retribución de las actividades de transporte y distribución de electricidad, y de transporte y distribución de gas natural y de las plantas de gas natural licuado, para lo que habrá de atenerse a las respectivas metodologías aprobadas conforme a lo previsto en el apartado anterior.

2. Supervisar la gestión y asignación de capacidad de interconexión, el tiempo utilizado por los transportistas y las empresas de distribución en efectuar conexiones y reparaciones, así como los mecanismos destinados a solventar la congestión de la capacidad en las redes.

A estos efectos, velará por la adecuada publicación de la información necesaria por parte de los gestores de red de transporte y, en su caso, de distribución, sobre las interconexiones, la utilización de la red y la asignación de capacidades a las partes interesadas.

3. Supervisar y, en su caso, certificar, la separación de las actividades de transporte, regasificación, distribución, almacenamiento y suministro en el sector del gas, y de las actividades de generación, transporte, distribución y suministro en el sector eléctrico, y en particular su separación funcional y la separación efectiva de cuentas con objeto de evitar subvenciones cruzadas entre dichas actividades.

4. Velar por el cumplimiento de la normativa y procedimientos que se establezcan relacionados con los cambios de suministrador.

5. En el sector del gas natural, supervisar las condiciones de acceso al almacenamiento, incluyendo el almacenamiento subterráneo, tanques de Gas Natural Licuado (GNL) y gas almacenado en los gasoductos, así como otros servicios auxiliares. Asimismo, supervisará el cumplimiento por parte de los propietarios de los requisitos que se establezcan para los almacenamientos no básicos de gas natural.

6. Supervisar las condiciones y tarifas de conexión aplicables a los nuevos productores de electricidad.

7. Supervisar los planes de inversión de los gestores de red de transporte, en particular, en lo que se refiere a su adecuación al plan de desarrollo de la red en el ámbito de la Unión Europea, pudiendo realizar recomendaciones para su modificación. La Comisión Nacional de los Mercados y la Competencia incluirá los resultados de dicha supervisión en su informe anual remitido a la Agencia de Cooperación de los Reguladores de la Energía y a la Comisión Europea.

Asimismo, la Comisión Nacional de los Mercados y la Competencia remitirá un informe a la propuesta del gestor de la red de transporte en el inicio de la planificación que refleje sus recomendaciones sobre las implicaciones económicas de las inversiones planeadas y su impacto en la sostenibilidad económico-financiera del sistema eléctrico y gasista.

De igual modo, en el trámite de audiencia a la propuesta de planificación, la Comisión Nacional de los Mercados y la Competencia informará al Ministerio para la Transición Ecológica sobre la planificación y el control de las inversiones, y señalará aquellos aspectos no considerados en su informe inicial, pudiendo convocarse la Comisión de Cooperación

para obtener un mejor entendimiento de la postura de la Comisión Nacional de los Mercados y la Competencia al respecto.

8. Velar por el respeto a la libertad contractual respecto de los contratos de suministro interrumpible y de los contratos a largo plazo siempre que sean compatibles con la legislación vigente y el Derecho de la Unión Europea.

9. Velar por el cumplimiento de las normas de seguridad y fiabilidad de las redes.

10. Velar por el cumplimiento, por los transportistas y distribuidores y, en su caso, por los propietarios de las redes y por los gestores de redes de transporte y distribución, de las obligaciones impuestas en la normativa aplicable, incluyendo las cuestiones transfronterizas. Asimismo, velará por la correcta aplicación por parte de los sujetos que actúen en los mercados de gas y electricidad de lo dispuesto en las disposiciones normativas de la Unión Europea.

11. Supervisar la adecuación de los precios y condiciones de suministro a los consumidores finales a lo dispuesto en la Ley 34/1998, de 7 de octubre, y en la Ley 54/1997, de 27 de noviembre, y sus normativas de desarrollo y publicar recomendaciones, al menos anualmente, para la adecuación de los precios de los suministros a las obligaciones de servicio público y a la protección de los consumidores.

12. Asegurar el acceso de los clientes a los datos de su consumo, en formato comprensible, armonizado y de forma rápida.

13. Determinar los sujetos a cuya actuación sean imputables deficiencias en el suministro a los usuarios, proponiendo las medidas que hubiera que adoptar.

14. Garantizar la transparencia y competencia en el sector eléctrico y en el sector del gas natural, incluyendo el nivel de los precios al por mayor, y velar por que las empresas de gas y electricidad cumplan las obligaciones de transparencia.

15. Supervisar el grado y la efectividad de la apertura del mercado y de competencia, tanto en el mercado mayorista como el minorista, incluidas entre otras, las reclamaciones planteadas por los consumidores de energía eléctrica y de gas natural, y las subastas reguladas de contratación a plazo de energía eléctrica.

A estos efectos, podrá tomar en consideración la información remitida por el Ministerio de Industria, Energía y Turismo a la que se hace referencia en la Disposición adicional octava.

16. Supervisar las inversiones en capacidad de generación que permita garantizar la seguridad del suministro.

17. Supervisar la relación entre el Gestor de Red Independiente y el propietario de las instalaciones, actuar como órgano de resolución de conflictos entre ambos, así como aprobar las inversiones del Gestor de Red Independiente.

18. Supervisar la cooperación técnica entre los gestores de las redes de transporte de energía eléctrica y gas y los gestores de terceros países.

19. Supervisar las medidas adoptadas por los gestores de la red de distribución para garantizar la exclusión de conductas discriminatorias.

20. Contribuir a la compatibilidad de los sistemas de intercambio de datos en los procesos de mercado a escala regional.

21. Determinar con carácter anual los operadores principales y dominantes, así como el resto de funciones relativas a dichos operadores de acuerdo con lo dispuesto en el Real Decreto-Ley 6/2000, de 23 de junio, de Medidas Urgentes de Intensificación de la Competencia en Mercados de Bienes y Servicios.

22. En relación con el déficit de las actividades reguladas y sus mecanismos de financiación, mantener y proporcionar la información que se determine, emitir los informes, declaraciones, certificaciones y comunicaciones que le sean requeridos, y realizar los cálculos necesarios en coordinación con el Ministerio de Industria, Energía y Turismo, así como asesorar técnicamente a la Comisión Interministerial del Fondo de Titulización del Déficit de Tarifa del Sistema Eléctrico conforme a lo dispuesto en la Disposición adicional vigésimo primera de la Ley 54/1997, de 27 de noviembre, y la normativa que desarrolla la regulación del proceso de gestión y titulización de los déficit del sistema eléctrico.

23. Gestionar el sistema de garantía de origen de la electricidad procedente de fuentes de energía renovables y de cogeneración de alta eficiencia.

24. Publicar los precios finales del mercado de electricidad, a partir de la información del operador del mercado y del operador del sistema.

25. En materia de protección al consumidor, gestionar el sistema de comparación de los precios del suministro de electricidad y gas natural sobre la base de las ofertas que realicen las empresas comercializadoras, así como la elaboración de informes que contengan la comparación y evolución de los precios del suministro de electricidad y gas y de los mercados minoristas.

26. Actuar como organismo supervisor de las subastas para la adquisición de gas natural para la fijación de la tarifa de último recurso, el gas talón de tanques y gasoductos y el gas colchón de almacenamientos subterráneos, así como de la capacidad de los almacenamientos básicos, cuando la normativa en la materia así lo disponga.

27. Elaborar los modelos normalizados de solicitud formal de acceso a las instalaciones del sistema gasista y de contratos de acceso, que propondrá a la Dirección General de Política Energética y Minas para su aprobación o modificación.

28. Elaborar los modelos normalizados para la publicación de la capacidad contratada y disponible, así como la metodología para su determinación, que propondrá a la Dirección General de Política Energética y Minas para su aprobación o modificación.

29. Aprobar el contrato entre el propietario de las instalaciones y el Gestor de Red Independiente en el que se detallen las condiciones contractuales así como las responsabilidades de cada uno.

30. Tramitar expedientes de exención de acceso de terceros a las instalaciones gasistas.

31. Emitir el preceptivo informe y propuesta en las autorizaciones para ejercer la comercialización de gas natural en los casos previstos en el artículo 80 de la Ley 34/1998, de 7 de octubre.

32. Inspeccionar el cumplimiento de los requisitos de los comercializadores de gas natural y de energía eléctrica, así como de los gestores de cargas y consumidores directos en mercado.

33. Calcular anualmente el saldo de mermas de cada red de transporte.

34. Emitir informe en los expedientes de autorización, modificación o cierre de instalaciones, en el proceso de planificación energética, en expedientes de aprobación o autorización de regímenes económicos o retributivos (sistemas eléctricos insulares y extrapeninsulares, distribución, transporte, instalaciones singulares, entre otros), en materia de calidad de suministro y de pérdidas, así como cuando sea requerido en materia de medidas eléctricas de acuerdo con lo dispuesto en la Ley 54/1997, de 27 de noviembre, y su normativa de desarrollo. Asimismo, en relación con las actividades de transporte y distribución, informará las propuestas de la retribución de las actividades.

35. Informar los expedientes de autorización, modificación, transmisión o cierre de instalaciones de la red básica de gas natural, así como en los procedimientos para su adjudicación. Emitir informes en relación a las condiciones de calidad de suministro y calidad de servicio, así como las consecuencias del incumplimiento de las mismas, las Normas de Gestión Técnica del Sistema y sus Protocolos de Detalle, costes de retribución de instalaciones y en los procesos de planificación de instalaciones de acuerdo con lo dispuesto en la Ley 34/1998, de 7 de octubre, y su normativa de desarrollo.

36. Dictar las circulares de desarrollo y ejecución de las normas contenidas en los reales decretos y órdenes del Ministro de Industria, Energía y Turismo que le habiliten para ello y que se dicten en desarrollo de la normativa energética.

37. Realizar cualesquiera otras funciones que le sean atribuidas por Ley o por Real Decreto.

38. Determinar las reglas de los mercados organizados en su componente normativa, en aquellos aspectos cuya aprobación corresponda a la autoridad regulatoria nacional, de conformidad con las normas del derecho comunitario europeo». Dichas reglas se publicarán en el “Boletín Oficial del Estado”.

39. Inspeccionar, a través de la Dirección de Energía, todas aquellas materias sobre las que la Comisión Nacional de los Mercados y la Competencia tenga atribuida competencia.

**Artículo 8.** *Supervisión y control del mercado postal.*

La Comisión Nacional de los Mercados y la Competencia supervisará y controlará el correcto funcionamiento del mercado postal. En particular, ejercerá las siguientes funciones:

1. Velar para que se garantice el servicio postal universal, en cumplimiento de la normativa postal y la libre competencia en el sector, ejerciendo las funciones y competencias que le atribuye la legislación vigente, sin perjuicio de lo indicado en la Disposición adicional undécima de esta Ley.
2. Verificar la contabilidad analítica del operador designado y el coste neto del servicio postal universal y determinar la cuantía de la carga financiera injusta de la prestación de dicho servicio de conformidad con lo establecido en el Capítulo III del Título III de la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal, así como en su normativa de desarrollo.
3. Gestionar el Fondo de financiación del servicio postal universal y las prestaciones de carácter público afectas a su financiación de conformidad con lo establecido en el Capítulo III del Título III de la Ley 43/2010, de 30 de diciembre, y en su normativa de desarrollo.
4. Supervisar y controlar la aplicación de la normativa vigente en materia de acceso a la red y a otras infraestructuras y servicios postales, de conformidad con lo establecido en el Título V de la Ley 43/2010, de 30 de diciembre, así como en su normativa de desarrollo.
5. Realizar el control y medición de las condiciones de prestación del servicio postal universal, de conformidad con lo establecido en el Capítulo II del Título III de la Ley 43/2010, de 30 de diciembre, así como en su normativa de desarrollo.
6. Gestionar y controlar la utilización del censo promocional conforme a lo definido en el artículo 31 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, conforme a lo que se determine reglamentariamente.
7. Dictar circulares para las entidades que operen en el sector postal, que serán vinculantes una vez publicadas en el «Boletín Oficial del Estado».
8. Emitir el informe previsto en la Disposición adicional segunda de la Ley 43/2010, de 30 de diciembre, para el seguimiento de las condiciones de prestación del servicio postal universal.
9. Realizar cualesquiera otras funciones que le sean atribuidas por Ley o por Real Decreto.

**Artículo 9.** *Supervisión y control en materia de mercado de comunicación audiovisual.*

La Comisión Nacional de los Mercados y la Competencia supervisará y controlará el correcto funcionamiento del mercado de comunicación audiovisual. En particular, ejercerá las siguientes funciones:

1. Elaborar y publicar un informe anual sobre la representación de las mujeres en los programas y contenidos audiovisuales, con especial atención a su representación en noticiarios y programas de contenido informativo de actualidad, en servicios de comunicación audiovisual de ámbito estatal, de acuerdo con lo previsto en el artículo 6.4 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.
2. Elaborar y publicar un informe cada tres años sobre las medidas de alfabetización mediática adoptadas por los prestadores del servicio de comunicación audiovisual de ámbito estatal y los prestadores del servicio de intercambio de vídeos a través de plataforma, de conformidad con lo previsto en el artículo 10.5 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.
3. Controlar y supervisar el cumplimiento de las obligaciones impuestas para garantizar la transparencia del régimen de propiedad de los prestadores del servicio de comunicación audiovisual de ámbito estatal y de los prestadores del servicio de intercambio de vídeos a través de plataforma conforme a lo dispuesto en el capítulo IV del título II de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.
4. Garantizar la libertad de recepción en territorio español de servicios audiovisuales cuyos titulares se encuentren establecidos en un Estado miembro de la Unión Europea, así como adoptar resoluciones para restringir la libertad de recepción en territorio español de un servicio de comunicación audiovisual televisivo procedente de otro Estado miembro de la Unión Europea o de un Estado parte del Convenio de Televisión Transfronteriza, de acuerdo

con lo dispuesto en el capítulo V del título II de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

5. Adoptar las medidas de salvaguarda cuando el prestador de un servicio de comunicación audiovisual televisivo sujeto a la jurisdicción de otro Estado miembro de la Unión Europea dirija su servicio total o principalmente al territorio español y se hubiera establecido en ese Estado miembro para eludir las normas españolas más estrictas, de conformidad con lo previsto en el capítulo V del título II de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

6. Vigilar el cumplimiento de la misión de servicio público encomendada a los prestadores del servicio público de comunicación audiovisual de ámbito estatal, así como la adecuación de los recursos públicos asignados para ello, de acuerdo con lo dispuesto en el título III de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

7. Supervisar y controlar el cumplimiento por los prestadores del servicio público de comunicación audiovisual de ámbito estatal de lo establecido en materia de ingresos procedentes de comunicaciones comerciales en la Ley 8/2009, de 28 de agosto, de financiación de la Corporación de Radio y Televisión Española.

8. Supervisar y controlar el cumplimiento de las obligaciones impuestas a los prestadores del servicio de comunicación audiovisual radiofónico de ámbito estatal y sonoro a petición, de acuerdo con lo previsto en el título IV de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

9. Supervisar y controlar el cumplimiento de las obligaciones impuestas a los prestadores del servicio de intercambio de vídeos a través de plataforma, de acuerdo con lo previsto en el título V de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

10. Controlar y supervisar el cumplimiento de las obligaciones de los prestadores del servicio de comunicación audiovisual televisivo de ámbito estatal, de conformidad con el título VI de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

11. **(Suprimido).**

12. Controlar y supervisar el cumplimiento de las obligaciones y los límites impuestos para la contratación en exclusiva de contenidos audiovisuales, la emisión de contenidos incluidos en el catálogo de acontecimientos de interés general y la compraventa de los derechos exclusivos en las competiciones futbolísticas españolas regulares, en los términos previstos en el título VII de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

13. Elaborar y publicar una memoria anual de las actuaciones realizadas por la Comisión Nacional de los Mercados y la Competencia en el ámbito audiovisual y un informe anual sectorial sobre el mercado audiovisual.

14. Supervisar la adecuación de los contenidos y comunicaciones comerciales audiovisuales con el ordenamiento vigente y con los códigos de autorregulación y corregulación, en los términos establecidos en el artículo 15 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

15. Promoción de la autorregulación y corregulación a nivel nacional, europeo e internacional, de acuerdo con lo establecido en los artículos 12, 14 y 15 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

16. Velar por el cumplimiento de los códigos de autorregulación y corregulación sobre contenidos audiovisuales verificando su conformidad con la normativa vigente, en los términos establecidos en los artículos 12, 14 y 15 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

17. Realizar cualesquiera otras funciones que le sean atribuidas por Ley o por Real Decreto.

**Artículo 10.** *Supervisión y control en materia de tarifas aeroportuarias.*

La Comisión Nacional de los Mercados y la Competencia ejercerá las siguientes funciones en materia de tarifas aeroportuarias:

1. Informar el Documento de Regulación Aeroportuaria (DORA) y sus modificaciones, así como acerca del cierre o enajenación de instalaciones o infraestructuras aeroportuarias,

conforme a lo previsto en la Ley 18/2014, de 15 de octubre, aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.

2. Supervisar el cumplimiento del procedimiento de transparencia y consulta llevado a cabo por Aena, S.A., y que las actualizaciones de sus tarifas aeroportuarias se ajustan al porcentaje que resulte de aplicar el ingreso máximo anual por pasajero ajustado (IMAAJ), conforme a lo previsto en la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia, y declarar la inaplicación de las modificaciones tarifarias establecidas por la entidad gestora del aeropuerto cuando las modificaciones tarifarias se hayan realizado incumpliendo lo previsto en dicha norma.

3. Dictar resoluciones vinculantes en relación con el procedimiento de transparencia y consulta que debe realizar Aena, S.A., conforme a lo previsto en la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.

4. Velar porque las tarifas aeroportuarias de Aena, S.A., no se apliquen de forma discriminatoria.

5. Resolver los conflictos entre Aena, S.A., y las asociaciones representativas de usuarios de los aeropuertos de la red en materia de tarifas aeroportuarias previstos en el artículo 12.c) o, en los términos en que se desarrolle reglamentariamente, los que pudieran plantear individualmente las compañías usuarias del aeropuerto.

6. Publicar un informe anual sobre su actividad como autoridad de supervisión en materia de tarifas aeroportuarias, en su caso, mediante la incorporación a la memoria anual.

7. Realizar cualesquiera otras funciones que le sean atribuidas por Ley o por Real Decreto.

**Artículo 11.** *Supervisión y control en el sector ferroviario.*

1. La Comisión Nacional de los Mercados y la Competencia supervisará y controlará el correcto funcionamiento del sector ferroviario y la situación de la competencia en los mercados de servicios ferroviarios, también, y en particular, en el mercado de transporte de viajeros en alta velocidad. En particular, ejercerá, bien por iniciativa propia, bien a solicitud de las autoridades competentes o partes interesadas, las siguientes funciones:

a) Salvaguardar la pluralidad de la oferta en la prestación de los servicios sobre la Red Ferroviaria de Interés General y sus zonas de servicio ferroviario, así como velar por que estos sean prestados en condiciones objetivas, transparentes y no discriminatorias.

b) Garantizar la igualdad entre empresas, así como entre cualesquiera candidatos, en las condiciones de acceso al mercado de los servicios ferroviarios.

c) Determinar, a petición de las autoridades competentes o de las empresas ferroviarias o candidatos interesados, que el objeto principal de un servicio internacional de transporte ferroviario de viajeros es transportar viajeros entre estaciones españolas y las de otros Estados miembros de la Unión Europea.

d) Determinar, a petición de las autoridades competentes, del administrador de la infraestructura, de las empresas ferroviarias o de los candidatos interesados, si está en peligro el equilibrio económico de un servicio de transporte sujeto a obligaciones de servicio público por la asignación de capacidad para realizar servicios de transporte ferroviario de viajeros total o parcialmente coincidentes. En caso de que decida que el equilibrio económico puede verse en peligro por causa del servicio de transporte de viajeros que pretenda explotar el candidato, indicará los cambios posibles que deban introducirse en el servicio que aseguren las condiciones para la concesión del derecho de acceso a la infraestructura.

e) Solicitar a los administradores de infraestructura, a gestores de instalaciones de servicio, a empresas ferroviarias y candidatos, así como a otras empresas involucradas en asuntos que deben ser verificados o comprobados por la Comisión Nacional de los Mercados y la Competencia, toda la información necesaria para el ejercicio de sus funciones, en particular, con la resolución de reclamaciones, supervisión del mercado ferroviario, fines estadísticos y observación del mercado. El plazo no podrá exceder de un mes salvo que, en circunstancias excepcionales, el órgano peticionario acuerde y autorice una prórroga limitada que no podrá exceder de dos semanas, siempre de conformidad con lo dispuesto por la Ley

39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

f) Solicitar a la Comisión Europea que examine las medidas específicas adoptadas por las autoridades nacionales en relación con el acceso a la infraestructura y a los servicios ferroviarios, la concesión de licencias, los cánones o la adjudicación de capacidad.

g) Realizar cualesquiera otras funciones que le sean atribuidas por ley o por norma reglamentaria.

h) Comprobar el cumplimiento de las disposiciones contables aplicables y las disposiciones sobre transparencia financiera establecidas en los apartados 3 y 4 del artículo 21 de la Ley 38/2015, de 29 de septiembre, del sector ferroviario, en el marco de la normativa ferroviaria, para lo cual podrá realizar o encargar la realización de auditorías a los administradores de infraestructuras, a los explotadores de instalaciones de servicio y, en su caso, a las empresas ferroviarias. En el caso de empresas integradas verticalmente, estas facultades se extenderán a todas las personas jurídicas.

Además, podrá también sacar conclusiones de las cuentas respecto de las cuestiones de las ayudas estatales, lo que informará a las autoridades competentes.

i) Velar por que los cánones y los precios privados establecidos por el administrador de infraestructuras cumplan lo dispuesto por el Derecho de la Unión Europea, la legislación del sector ferroviario y su normativa de desarrollo y por que no sean discriminatorios.

2. Igualmente, en el marco de las funciones recogidas en el apartado anterior, la Comisión Nacional de los Mercados y la Competencia supervisará y controlará, por iniciativa propia, las actividades de los administradores de infraestructuras ferroviarias y, cuando proceda, las de los explotadores de instalaciones de servicio y empresas ferroviarias, en relación con los siguientes asuntos:

a) la declaración sobre la red, en sus versiones provisional y definitiva, así como los criterios establecidos en la misma, y en particular comprobará si contiene cláusulas discriminatorias u otorga poderes discrecionales al administrador de infraestructuras que este pueda utilizar para discriminar a los candidatos;

b) el sistema, la cuantía o estructura de cánones, tarifas y precios por la utilización de infraestructuras y servicios;

c) autorizar al administrador de infraestructuras ferroviarias a la continuidad del cobro de cánones en el caso de una infraestructura declarada congestionada en la que las medidas definidas en el plan de aumento de capacidad no avanzan, bien por razones ajenas al control del administrador de infraestructuras o bien porque las opciones posibles no son viables desde el punto de vista económico o financiero;

d) el proceso de consulta previo a la fijación de cánones y tarifas entre empresas ferroviarias o candidatos y los administradores de infraestructuras e intervenir cuando prevea que el resultado de dicho proceso puede contravenir las disposiciones vigentes;

e) las disposiciones sobre acceso a la infraestructura y a los servicios ferroviarios, así como el procedimiento de adjudicación y sus resultados;

f) gestión del tráfico;

g) planificación de la renovación y mantenimiento programado o no programado;

h) cumplimiento de los requisitos del administrador de infraestructuras ferroviarias, incluidos los relativos a los conflictos de intereses, independencia de sus funciones esenciales, imparcialidad del administrador de las infraestructuras ferroviarias respecto a la gestión del tráfico y a la planificación del mantenimiento, así como la externalización y compartición de las funciones del administrador de las infraestructuras ferroviarias.

3. La Comisión Nacional de los Mercados y la Competencia estudiará todas las denuncias y, en su caso, solicitará información pertinente e iniciará un proceso de consulta a todas las partes interesadas en el plazo de un mes desde de la recepción de la denuncia. Resolverá acerca de cualquier denuncia, tomará medidas para remediar la situación y comunicará a las partes interesadas su decisión motivada en un plazo de tiempo prudencial previamente fijado, y, en cualquier caso, en un plazo de seis semanas a partir de la recepción de toda la información pertinente. Sin perjuicio de las facultades de las autoridades de competencia nacionales en materia de protección de la competencia en los mercados de servicios ferroviarios, la Comisión Nacional de los Mercados y de la

Competencia decidirá por iniciativa propia, cuando corresponda, las medidas adecuadas para corregir discriminaciones en perjuicio de los candidatos, distorsiones del mercado y otras situaciones indeseables en estos mercados, en particular respecto a lo dispuesto en los números 1.º a 9.º del apartado 1.f) del artículo 12.

4. En el ejercicio de la función de cooperación, a fin de supervisar la competencia en el mercado y coordinar los servicios de transporte ferroviario internacional, la Comisión Nacional de los Mercados y la Competencia llevará a cabo, entre otras, las siguientes tareas:

a) participará y colaborará en una red de reguladores ferroviarios coordinada por la Comisión Europea;

b) cooperará estrechamente con el resto de organismos reguladores, mediante acuerdos de trabajo, con fines de asistencia mutua en sus tareas de supervisión del mercado y tratamiento de reclamaciones o investigaciones;

c) cooperará con el resto de organismos reguladores para elaborar principios y prácticas comunes, incluidas disposiciones, para la toma de las decisiones en relación con las funciones recogidas en este artículo, así como para la resolución de los conflictos que surjan en los servicios internacionales;

d) intercambiará información con el resto de organismos reguladores acerca de su trabajo y de sus motivos y prácticas en la toma de decisiones y en particular sobre los principales aspectos de los procedimientos y los problemas de interpretación de la legislación de la Unión en el ámbito ferroviario incorporada a los ordenamientos nacionales, y cooperarán de otras maneras a fin de coordinar sus tomas de decisiones en el conjunto de la Unión;

e) cooperará, en el marco de sus funciones reconocidas en este artículo, con otros organismos reguladores afectados sobre cuestiones relacionadas con servicios internacionales, a fin de preparar sus respectivas decisiones y llegar a adoptar una resolución sobre la cuestión;

f) cooperará y consultará a los organismos reguladores de todos los Estados miembros, si procede a la Comisión Europea, en el caso de reclamaciones, o de investigaciones por iniciativa propia, sobre cuestiones de acceso o tarifación relacionadas con una franja internacional y, así como en relación con la supervisión de la competencia en el mercado de los servicios de transporte ferroviario internacional, y les pedirá toda la información necesaria antes de tomar su decisión. A su vez, cuando la Comisión Nacional de los Mercados y la Competencia sea consultada a efectos del tratamiento de una reclamación o investigación en una franja internacional deberá aportar toda la información que tenga derecho a solicitar a su vez en virtud del ordenamiento jurídico español;

g) en caso de que la Comisión Nacional de los Mercados y la Competencia reciba una reclamación, o efectúe una investigación por iniciativa propia, transmitirá la información pertinente al organismo regulador competente;

h) podrá revisar las decisiones y prácticas de las asociaciones de administradores de infraestructuras en materia de cánones o adjudicación de capacidad en relación con el transporte ferroviario internacional.

i) cooperará con los reguladores ferroviarios de otros estados de la Unión Europea en relación a infraestructuras de titularidad compartida, cuando los Estados concernidos así lo acuerden, a fin de unificar las consecuencias de sus decisiones.

5. La Comisión Nacional de los Mercados y la Competencia consultará de forma periódica, y en cualquier caso al menos una vez cada dos años, a los representantes de los usuarios de los servicios de transporte ferroviario de mercancías y viajeros para tener en cuenta sus puntos de vista sobre el mercado ferroviario en el desarrollo de sus funciones.

**Artículo 12.** *Resolución de conflictos.*

1. La Comisión Nacional de los Mercados y la Competencia resolverá los conflictos que le sean planteados por los operadores económicos en los siguientes casos:

a) En los mercados de comunicaciones electrónicas, la Comisión Nacional de los Mercados y la Competencia resolverá los conflictos que se susciten en relación con las obligaciones existentes en virtud de la Ley 32/2003, de 3 de noviembre, y su normativa de desarrollo, entre operadores o entre operadores y otras entidades que, de conformidad con

lo establecido en la citada Ley, se beneficien de las obligaciones de acceso e interconexión, de acuerdo con la definición que se da a los conceptos de acceso e interconexión en el Anexo II de dicha Ley. En particular, resolverá:

1.º Los conflictos en materia de acceso, interconexión e interoperabilidad derivados de obligaciones que en su caso resulten de las actuaciones a que se refieren los apartados 3 y 4 del artículo 11 de la Ley 32/2003, de 3 de noviembre, así como de las obligaciones específicas a que se refiere el artículo 13 de dicha Ley.

2.º Los conflictos entre operadores en relación con la forma de sufragar los costes que produzca la conservación de los números telefónicos a que se refiere el artículo 18 de la Ley 32/2003, de 3 de noviembre.

3.º Los conflictos entre operadores en relación con las condiciones de uso compartido a que se refiere el artículo 30 de la Ley 32/2003, de 3 de noviembre.

4.º Los conflictos que se produzcan entre prestadores de servicios de consulta telefónica y operadores de redes públicas telefónicas fijas, de acuerdo con la Orden CTE/711/2002, de 26 de marzo, por la que se establecen las condiciones de prestación del servicio de consulta telefónica sobre números de abonado.

5.º Los conflictos que surjan sobre las condiciones en las que se ofertará el servicio mayorista de acceso a bandas de frecuencias de conformidad con el artículo 4.6 del Real Decreto 458/2011, de 1 de abril, sobre actuaciones en materia de espectro radioeléctrico para el desarrollo de la sociedad digital.

6.º Los conflictos en materia de itinerancia.

7.º Los conflictos transfronterizos entre prestadores de redes o servicios de comunicaciones electrónicas en el que una de las partes esté radicada en otro Estado miembro de la Unión Europea, a que se refiere el artículo 14.2 de la Ley 32/2003, de 3 de noviembre.

8.º Los conflictos que sobre la gestión del múltiple digital surjan entre los prestadores de los servicios de comunicación audiovisual.

b) En los mercados de la electricidad y del gas, la Comisión Nacional de los Mercados y la Competencia resolverá los siguientes conflictos:

1.º Conflictos que le sean planteados respecto a los contratos relativos al acceso de terceros a las redes de transporte y, en su caso, distribución, en los términos que reglamentariamente se establezcan.

2.º Conflictos que le sean planteados en relación con la gestión económica y técnica del sistema y el transporte, incluyendo las conexiones entre instalaciones.

c) En materia de tarifas aeroportuarias, la Comisión Nacional de los Mercados y la Competencia resolverá los recursos frente a las decisiones de Aena, S.A., relativas a la modificación del sistema o nivel de sus tarifas aeroportuarias, que interpongan las asociaciones representativas de usuarios de la red de aeropuertos de Aena, S.A., o, en los términos en que se desarrolle reglamentariamente, los que pudieran plantear individualmente las compañías usuarias del aeropuerto. La Comisión acumulará la tramitación de los recursos presentados.

A estos efectos se consideran asociaciones representativas de usuarios de la red de aeropuertos de Aena, S.A., las definidas en el artículo 19, letra d) de la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.

Esta resolución incluirá la modificación tarifaria revisada que proceda, que sustituirá al contenido de la decisión de Aena, S.A., y, en su caso, los estándares que se correspondan con los indicadores y niveles de calidad de servicio que considere aceptables y consistentes con la modificación tarifaria revisada.

La modificación tarifaria revisada de la Comisión Nacional de los Mercados y de la Competencia deberá respetar el ingreso máximo anual por pasajero ajustado (IMAAJ) que resulte de aplicar las correcciones establecidas en el artículo 33 de la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia, al ingreso máximo anual por pasajero (IMAP) adoptado para el ejercicio en el Documento de Regulación Aeroportuaria (DORA).

En este procedimiento la Comisión verificará que la decisión de Aena, S.A., se ha producido conforme al procedimiento establecido en la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia, se ajusta a los requisitos establecidos en el Documento de Regulación Aeroportuaria (DORA), garantiza la sostenibilidad de la red y la accesibilidad a los aeropuertos integrados en ella, así como a la suficiencia de ingresos, responde a los principios de no discriminación, objetividad, eficiencia y transparencia, resulta justificada, de acuerdo con las previsiones del Documento de Regulación Aeroportuaria (DORA) en materia de previsiones de tráfico e inversiones, y los requerimientos y necesidades de las compañías usuarias de los aeropuertos.

d) En el mercado postal, la Comisión Nacional de los Mercados y la Competencia resolverá sobre:

1.º Conflictos, de conformidad con lo establecido en el artículo 48 de la Ley 43/2010, de 30 de diciembre, entre el operador designado para prestar el servicio postal universal y otros operadores postales que prestan servicios en el ámbito del servicio postal universal respecto al acceso a la red postal y a otros elementos de infraestructura y servicios postales.

2.º Establecimiento, de conformidad con lo previsto en el artículo 45.3 de la Ley 43/2010, de 30 de diciembre, a petición del operador interesado, de las condiciones de acceso a la red postal si las negociaciones entre titulares de autorizaciones singulares y el operador designado no hubieran concluido en la celebración de un contrato.

3.º Conflictos, de conformidad con lo establecido en el artículo 49 de la Ley 43/2010, de 30 de diciembre, que se planteen entre operadores postales no designados para la prestación del servicio postal universal.

e) En el mercado de comunicación audiovisual, la Comisión Nacional de los Mercados y la Competencia resolverá los siguientes conflictos:

1.º Los conflictos que se susciten entre los agentes intervinientes en los mercados de comunicación audiovisual sobre materias en las que la Comisión tenga atribuida competencia.

2.º Los conflictos que se susciten en relación con el acceso a estadios y recintos deportivos por los prestadores de servicios de comunicación audiovisual radiofónica a que se refiere el artículo 145 de la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual.

f) En el sector ferroviario, corresponde a la Comisión Nacional de los Mercados y la Competencia en exclusiva conocer y resolver las reclamaciones que presenten las empresas ferroviarias y los restantes candidatos en relación con la actuación del administrador de infraestructuras ferroviarias, los explotadores de instalaciones de servicio o prestadores de los servicios, así como las empresas ferroviarias y restantes candidatos, y que versen, en particular, sobre:

1.º El contenido y la aplicación de las declaraciones sobre la red.

2.º Los procedimientos de adjudicación de capacidad y sus resultados.

3.º La cuantía, la estructura o la aplicación de los cánones, tarifas y precios que se les exijan o puedan exigírseles.

4.º Cualquier trato discriminatorio en el acceso a las infraestructuras o a las instalaciones de servicio, y en relación con los servicios que en ellas se llevan a cabo.

5.º La prestación de servicios en los corredores ferroviarios internacionales de transporte de mercancías.

6.º Las reclamaciones o investigaciones relacionadas con una franja internacional cuando proceda conocer y resolver a ella y, en los demás casos, cooperará con los órganos reguladores del mercado ferroviario de los demás Estados miembros de la Unión Europea competentes con la franja internacional.

7.º La gestión del tráfico.

8.º La planificación de la renovación y mantenimiento programado o no programado.

9.º El cumplimiento de los requisitos del administrador de infraestructuras ferroviarias, incluidos los relativos a los conflictos de intereses, independencia de sus funciones esenciales, imparcialidad del administrador de las infraestructuras ferroviarias respecto a la

gestión del tráfico y a la planificación del mantenimiento, así como la externalización y compartición de las funciones del administrador de las infraestructuras ferroviarias.

Las reclamaciones deberán presentarse en el plazo de un mes desde que se produzca el hecho o la decisión correspondiente. La Comisión Nacional de los Mercados y la Competencia solicitará la información relevante e iniciará las consultas con todas las partes implicadas dentro del plazo de un mes a partir de recibo de la reclamación. En caso de una reclamación contra la negativa de otorgar capacidad de infraestructura, o contra los términos en que esta se otorga, resolverá para confirmar la decisión del administrador de la infraestructura o de la instalación de servicio, o bien para requerir la modificación de esa decisión de conformidad con las instrucciones específicas que se consideren apropiadas.

2. En la resolución de los conflictos a que hace referencia el apartado anterior, la Comisión resolverá acerca de cualquier denuncia y adoptará, a petición de cualquiera de las partes, una resolución para resolver el litigio lo antes posible y, en todo caso, en el plazo de tres meses desde la recepción de toda la información. En el supuesto de resolución de conflictos a que hace referencia el epígrafe f) del número 1 anterior, el plazo máximo será de 6 semanas.

La resolución que dicte la Comisión Nacional de los Mercados y la Competencia en los casos previstos en el apartado anterior será vinculante para las partes sin perjuicio de los recursos que procedan de acuerdo con lo dispuesto en el artículo 36 de esta ley.

## CAPÍTULO III

## Organización y funcionamiento

**Artículo 13.** *Órganos de gobierno.*

La Comisión Nacional de los Mercados y la Competencia ejercerá sus funciones a través de los siguientes órganos de gobierno:

a) El Consejo de la Comisión Nacional de los Mercados y la Competencia.

b) El Presidente de la Comisión Nacional de los Mercados y la Competencia, que lo será también de su Consejo.

**Artículo 14.** *El Consejo.*

1. El Consejo es el órgano colegiado de decisión en relación con las funciones resolutorias, consultivas, de promoción de la competencia y de arbitraje y de resolución de conflictos atribuidas a la Comisión Nacional de los Mercados y la Competencia, sin perjuicio de las delegaciones que pueda acordar.

En todo caso, son facultades indelegables del Consejo la aprobación del anteproyecto de presupuestos del organismo, de su memoria anual y sus planes anuales o plurianuales de actuación en que se definan sus objetivos y sus prioridades, la aprobación del reglamento de funcionamiento interno, el nombramiento del personal directivo, la impugnación de actos y disposiciones a los que se refiere el artículo 5.4 de esta Ley y, en su caso, la potestad de dictar circulares y comunicaciones de carácter general a los agentes del mercado objeto de regulación o supervisión en cada caso.

2. El Consejo de la Comisión Nacional de los Mercados y la Competencia está integrado por diez miembros.

3. A las reuniones del Consejo podrá asistir, con voz pero sin voto, el personal directivo de la Comisión y cualquier integrante del personal no directivo que determine el Presidente, de acuerdo con los criterios generales que a tal efecto acuerde el Consejo. No podrán asistir a las reuniones del Consejo los miembros del Gobierno ni los altos cargos de las Administraciones Públicas.

**Artículo 15.** *Nombramiento y mandato de los miembros del Consejo.*

1. Los miembros del Consejo, y entre ellos el Presidente y el Vicepresidente, serán nombrados por el Gobierno, mediante Real Decreto, a propuesta del Ministro de Economía y Competitividad, entre personas de reconocido prestigio y competencia profesional en el

ámbito de actuación de la Comisión, previa comparecencia de la persona propuesta para el cargo ante la Comisión correspondiente del Congreso de los Diputados. El Congreso, a través de la Comisión competente y por acuerdo adoptado por mayoría absoluta, podrá vetar el nombramiento del candidato propuesto en el plazo de un mes natural a contar desde la recepción de la correspondiente comunicación. Transcurrido dicho plazo sin manifestación expresa del Congreso, se entenderán aceptados los correspondientes nombramientos.

2. El mandato de los miembros del Consejo será de seis años sin posibilidad de reelección. La renovación de los miembros del Consejo se hará parcialmente cada dos años, de modo que ningún miembro del Consejo permanezca en su cargo por tiempo superior a seis años.

**Artículo 16.** *Funcionamiento del Consejo.*

1. El Consejo actúa en pleno o en sala. La asistencia de los miembros del Consejo a las reuniones del Consejo es obligatoria, salvo casos debidamente justificados.

Los acuerdos se adoptarán por mayoría de votos de los asistentes. En caso de empate decidirá el voto de quien presida la reunión.

2. A propuesta del Presidente, el Consejo en pleno, elegirá un Secretario no consejero, que deberá ser licenciado en derecho o titulación que lo sustituya y funcionario de carrera perteneciente a un cuerpo del subgrupo A1, al servicio de la Administración General del Estado, que tendrá voz pero no voto, al que corresponderá asesorar al Consejo en derecho, informar sobre la legalidad de los asuntos sometidos a su consideración, así como las funciones propias de la secretaría de los órganos colegiados. El servicio jurídico del organismo dependerá de la Secretaría del Consejo.

3. El régimen de funcionamiento del Consejo en pleno y salas se desarrollará en el Reglamento de funcionamiento interno, que será aprobado por el pleno según lo dispuesto en el artículo 26.4.

**Artículo 17.** *El pleno del Consejo.*

1. El Consejo en pleno está integrado por todos los miembros del Consejo. Lo preside el Presidente de la Comisión Nacional de los Mercados y la Competencia. En caso de vacante, ausencia o enfermedad del Presidente, le suplirá el Vicepresidente o en su defecto, el consejero de mayor antigüedad y, a igualdad de antigüedad, el de mayor edad.

2. El pleno del Consejo se entenderá válidamente constituido con la asistencia del Presidente o persona que lo sustituya, el Secretario, y cinco miembros del Consejo.

**Artículo 18.** *Las salas del Consejo.*

1. El Consejo consta de dos salas, una dedicada a temas de competencia y otra a supervisión regulatoria.

2. Cada una de las salas estará compuesta por cinco miembros del Consejo. La Sala de Competencia estará presidida por el Presidente de la Comisión Nacional de los Mercados y la Competencia y la de Supervisión regulatoria por el Vicepresidente. El Consejo en pleno determinará la asignación de los miembros del Consejo a cada sala y, en los términos establecidos reglamentariamente, aprobará y publicará el régimen de rotación entre salas de los consejeros, incluyendo los criterios de selección y periodicidad de las rotaciones. Cuando concurran circunstancias excepcionales que lo justifiquen, podrá adoptar otras medidas tendentes a garantizar el adecuado funcionamiento de las salas.

3. La convocatoria de las salas corresponde a su Presidente, por propia iniciativa o a petición de, al menos, la mitad de los consejeros.

4. Las salas del Consejo se entenderán válidamente constituidas con la asistencia de su Presidente, o persona que le sustituya, el Secretario del Consejo y, al menos, dos consejeros.

**Artículo 19.** *Funciones del Presidente.*

1. Corresponde al Presidente de la Comisión Nacional de los Mercados y la Competencia:

a) Ejercer, en general, las competencias que a los presidentes de los órganos colegiados administrativos atribuye la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

b) Convocar al Consejo en pleno por propia iniciativa o a petición de, al menos, la mitad de los consejeros, y presidirlo.

c) Ostentar la representación legal e institucional de la Comisión.

d) Velar por el adecuado desarrollo de las actuaciones de la Comisión, de acuerdo con el ordenamiento jurídico.

e) Mantener el buen orden y gobierno de la organización de la Comisión.

f) Impulsar la actuación de la Comisión y el cumplimiento de las funciones que tenga encomendadas. En particular, la propuesta de los planes anuales o plurianuales de actuación, en los que se definan sus objetivos y prioridades.

g) Ejercer funciones de jefatura del personal de la Comisión, de acuerdo con las competencias atribuidas por su legislación específica.

h) Dirigir, coordinar, evaluar y supervisar las distintas unidades de la Comisión, sin perjuicio de las funciones del Consejo; en particular coordinar, con la asistencia del Secretario del Consejo, el correcto funcionamiento de las unidades de la Comisión.

i) Dar cuenta al titular del Ministerio de adscripción de las vacantes que se produzcan en el Consejo de la Comisión Nacional de los Mercados y la Competencia.

j) Aprobar los actos de ejecución de los presupuestos de la Comisión.

k) Ejercer las competencias que le correspondan en la contratación de la Comisión.

l) Cuantas funciones le delegue el Consejo.

m) Efectuar la rendición de cuentas de la Comisión, de acuerdo con la Ley 47/2003, de 26 de noviembre.

n) Comparecer ante el Parlamento en los términos previstos en esta Ley.

o) Ostentar la presidencia del Consejo de Defensa de la Competencia.

p) Cualesquiera otras que le atribuya el Estatuto al que se refiere el artículo 26 o el Reglamento de funcionamiento interno.

2. En caso de vacante, ausencia o enfermedad, el Presidente será sustituido en el ejercicio de sus funciones por el Vicepresidente.

**Artículo 20.** *Funciones del Consejo de la Comisión Nacional de los Mercados y la Competencia.*

El Consejo de la Comisión Nacional de los Mercados y la Competencia es el órgano de decisión en relación con las funciones resolutorias, consultivas, de promoción de la competencia y de arbitraje y de resolución de conflictos previstas en esta Ley. En particular, es el órgano competente para:

1. Resolver y dictaminar los asuntos que la Comisión Nacional de los Mercados y la Competencia tiene atribuidos por esta Ley y por el resto de la legislación vigente.

2. Resolver los procedimientos sancionadores previstos en la legislación sectorial y en la Ley 15/2007, de 3 de julio, y sus normas de desarrollo cuando no correspondan a otros órganos de la Administración General del Estado.

3. Solicitar o acordar el envío de expedientes de control de concentraciones que entren en el ámbito de aplicación de la Ley 15/2007, de 3 de julio, a la Comisión Europea, según lo previsto en los artículos 9 y 22 del Reglamento (CE) n.º 139/2004 del Consejo, de 20 de enero, sobre el control de las concentraciones entre empresas.

4. Acordar el levantamiento de la obligación de suspensión de la ejecución de una concentración económica, de conformidad con el artículo 9.6 de la Ley 15/2007, de 3 de julio.

5. Resolver sobre el cumplimiento de las resoluciones y decisiones en materia de conductas prohibidas y de concentraciones.

6. Adoptar las comunicaciones previstas en el artículo 30.3 de esta Ley, así como las declaraciones de inaplicabilidad previstas en el artículo 6 de la Ley 15/2007, de 3 de julio.

7. Aprobar las circulares previstas en esta Ley.

8. Interesar la instrucción de expedientes.

9. Adoptar los informes a que se refieren las letras a), b) y c) del artículo 5.2 de esta Ley, los informes, estudios y trabajos sobre sectores económicos y en materia de competencia y los informes en materia de ayudas públicas.

10. Acordar la impugnación de los actos y disposiciones a los que se refiere el artículo 5.4 de esta Ley.

11. Aprobar su Reglamento de funcionamiento interno, en el cual se establecerá su funcionamiento administrativo y la organización de sus servicios.

12. Resolver sobre las recusaciones, y correcciones disciplinarias del Presidente, Vicepresidente y consejeros y apreciar la incapacidad y el incumplimiento grave de sus funciones.

13. Nombrar y acordar el cese del personal directivo, a propuesta del Presidente del Consejo.

14. Nombrar y acordar el cese del Secretario, a propuesta del Presidente del Consejo.

15. Aprobar el anteproyecto de presupuesto y formular las cuentas del organismo.

16. Aprobar la memoria anual del organismo, así como los planes anuales o plurianuales de actuación en los que se definan objetivos y prioridades.

**Artículo 21.** *Competencias de pleno y salas.*

1. El pleno del Consejo de la Comisión Nacional de los Mercados y la Competencia conocerá de los siguientes asuntos:

a) Los que, de acuerdo con lo dispuesto por el artículo 14.1 de la presente Ley, sean indelegables para el Consejo, con la excepción de la impugnación de actos y disposiciones a los que se refiere el artículo 5.4.

b) Aquellos en que se manifieste una divergencia de criterio entre la Sala de Competencia y la de Supervisión regulatoria.

c) Los asuntos que por su especial incidencia en el funcionamiento competitivo de los mercados o actividades sometidos a supervisión, recabe para sí el pleno, por mayoría de seis votos y a propuesta del Presidente o de tres miembros del Consejo.

2. Las salas conocerán de los asuntos que no estén expresamente atribuidos al pleno. Reglamentariamente se determinarán los supuestos en los que, correspondiendo el conocimiento de un asunto a una de las salas, deba informar la otra con carácter preceptivo. En todo caso, deberá emitirse informe en los siguientes asuntos:

a) Por la Sala de Competencia, en los procedimientos que, previstos en los artículos 6 a 11 de esta Ley, afecten al grado de apertura, la transparencia, el correcto funcionamiento y la existencia de una competencia efectiva en los mercados.

b) Por la Sala de Supervisión regulatoria, en los procedimientos en materia de defensa de la competencia previstos por el artículo 5 de esta Ley que estén relacionados con los sectores a los que se refieren los artículos 6 a 11.

**Artículo 22.** *Funciones e incompatibilidades de los miembros del Consejo.*

1. Los miembros del Consejo de la Comisión Nacional de los Mercados y la Competencia ejercerán su función con dedicación exclusiva y tendrán la consideración de altos cargos de la Administración General del Estado.

2. Los miembros del Consejo no podrán asumir individualmente funciones ejecutivas o de dirección de áreas concretas de la Comisión Nacional de los Mercados y la Competencia que correspondan al personal directivo de la Comisión.

3. Los miembros del Consejo estarán sometidos al régimen de incompatibilidad de actividades establecido para los altos cargos de la Administración General del Estado en la Ley 5/2006, de 10 de abril, de regulación de los conflictos de intereses de los miembros del Gobierno y de los Altos Cargos de la Administración General del Estado, y en sus disposiciones de desarrollo.

4. Durante los dos años posteriores a su cese, el Presidente, el Vicepresidente y los consejeros no podrán ejercer actividad profesional privada alguna relacionada con los sectores regulados y la actividad de la Comisión Nacional de los Mercados y la Competencia.

En virtud de esta limitación, el Presidente, el Vicepresidente y los consejeros de esta Comisión, al cesar en su cargo por renuncia, expiración del término de su mandato o incapacidad permanente para el ejercicio de sus funciones, tendrán derecho a percibir, a partir del mes siguiente a aquel en que se produzca su cese y durante un plazo igual al que hubieran desempeñado su cargo, con el límite máximo de dos años, una compensación económica mensual igual a la doceava parte del ochenta por ciento del total de retribuciones asignadas al cargo respectivo en el presupuesto en vigor durante el plazo indicado.

No habrá lugar a la percepción de dicha compensación en caso de desempeño, de forma remunerada, de cualquier puesto de trabajo, cargo o actividad en el sector público o privado en los términos previstos en el artículo 1 del Real Decreto-Ley 20/2012, de 13 de julio, de medidas para garantizar la estabilidad presupuestaria y de fomento de la competitividad.

**Artículo 23.** *Causas de cese en el ejercicio del cargo.*

1. Los miembros del Consejo cesarán en su cargo:

a) Por renuncia aceptada por el Gobierno.
b) Por expiración del término de su mandato.
c) Por incompatibilidad sobrevenida.
d) Por haber sido condenado por delito doloso.
e) Por incapacidad permanente.
f) Mediante separación acordada por el Gobierno por incumplimiento grave de los deberes de su cargo o el incumplimiento de las obligaciones sobre incompatibilidades, conflictos de interés y del deber de reserva. La separación será acordada por el Gobierno, con independencia del régimen sancionador que en su caso pudiera corresponder, previa instrucción de expediente por el titular del Ministerio de Economía y Competitividad.

2. Si durante el período de duración del mandato correspondiente a un determinado Consejero se produjera su cese, el sucesor será nombrado por el tiempo que restase al sustituido para la terminación de su mandato. Si el cese se hubiera producido una vez transcurridos cuatro años desde el nombramiento, no resultará de aplicación el límite anterior, y el sucesor será nombrado por el periodo de seis años previsto con carácter general.

3. Continuarán desempeñando su cargo en funciones los miembros del Consejo en los que concurran las causas de cese contempladas en las letras a) y b) del apartado 1 hasta que se publique en el «Boletín Oficial del Estado» el real decreto de cese correspondiente.

**Artículo 24.** *Obligación de informar y garantías para la actuación imparcial.*

1. El Presidente, el Vicepresidente, los consejeros, directivos y empleados, o sus representantes, que hayan prestado servicios profesionales en entidades de un mercado o sector en el que la Comisión Nacional de los Mercados y la Competencia ejerce su supervisión, deberán notificar al Consejo cualquier derecho o facultad, cualquiera que sea su denominación, a reserva o recuperación de las relaciones profesionales, a indemnizaciones o a cualesquiera ventajas de contenido patrimonial. En el caso de los miembros del Consejo dicha circunstancia deberá hacerse pública.

2. En aplicación de los principios de independencia y objetividad, la Comisión Nacional de los Mercados y la Competencia garantizará que sus empleados cuenten en sus actuaciones y en los procedimientos en que intervengan con reglas objetivas, predeterminadas y que delimiten adecuadamente las responsabilidades que les incumben.

**Artículo 25.** *Órganos de dirección.*

1. La Comisión Nacional de los Mercados y la Competencia contará con cuatro direcciones de instrucción a las que les corresponderá el ejercicio de las funciones señaladas en este artículo, además de aquellas que les pudiera delegar el Consejo, a excepción de las funciones de desarrollo normativo y de resolución y dictamen que dicho órgano tiene atribuidas de conformidad con el artículo 20 de esta Ley:

a) La Dirección de Competencia, a la que le corresponderá la instrucción de los expedientes relativos a las funciones previstas en el artículo 5 de esta Ley.

b) La Dirección de Telecomunicaciones y del Sector Audiovisual, a la que corresponderá la instrucción de los expedientes relativos a las funciones previstas en los artículos 6, 9 y 12.1.a) y e) de esta Ley.

c) La Dirección de Energía, a la que corresponderá la instrucción de los expedientes relativos a las funciones previstas en los artículos 7 y 12.1.b) de esta Ley.

d) La Dirección de Transportes y del Sector Postal, a la que corresponderá la instrucción de los expedientes relativos a las funciones previstas en los artículos 8, 10, 11 y 12.1.c), d) y f) de esta Ley.

2. Las Direcciones mencionadas en el apartado anterior ejercerán sus funciones de instrucción con independencia del Consejo.

3. Los titulares de las Direcciones de instrucción ejercerán sus funciones con dedicación exclusiva y estarán sometidos al régimen de incompatibilidades de actividades establecido para los altos cargos en la Ley 5/2006, de 10 de abril, y en sus disposiciones de desarrollo.

Su régimen de nombramiento y cese será el establecido para el personal directivo, según lo dispuesto en el artículo 26.3 de esta Ley.

**Artículo 26.** *Estatuto Orgánico y Reglamento de funcionamiento interno.*

1. El Gobierno aprobará, mediante real decreto, el Estatuto Orgánico de la Comisión Nacional de los Mercados y la Competencia.

2. El Estatuto Orgánico determinará la distribución de asuntos en el Consejo entre el pleno y las salas y las funciones y la estructura interna de las Direcciones de instrucción y demás áreas de responsabilidad, cualquiera que sea su denominación, al frente de las cuales se designará al personal directivo.

3. Corresponde al personal directivo la dirección, la organización, impulso y cumplimiento de las funciones encomendadas al área a cuyo frente se encuentre, de acuerdo con las instrucciones emanadas del Consejo y del Presidente de la Comisión, sin perjuicio de la debida separación entre las funciones de instrucción y resolución en procedimientos sancionadores.

El personal directivo de otras áreas de responsabilidad diferentes a las Direcciones de instrucción, será nombrado y cesado por el pleno del Consejo de la Comisión Nacional de los Mercados y la Competencia a propuesta de su Presidente. La selección se realizará mediante convocatoria pública y con procedimientos basados en los principios de igualdad, mérito y capacidad, de acuerdo con lo previsto en el artículo 13.2 de la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público, y de acuerdo con lo establecido en el artículo 31.5 de esta Ley.

4. El pleno del Consejo de la Comisión Nacional de los Mercados y la Competencia aprobará el Reglamento de funcionamiento interno del organismo, en el que se regulará, respetando lo dispuesto en el Estatuto Orgánico de la Comisión Nacional de los Mercados y la Competencia, la actuación de sus órganos, la organización del personal, el régimen de transparencia y de reserva de la información y, en particular, el funcionamiento del Consejo, incluyendo el régimen de convocatorias y sesiones del pleno y de las salas y el procedimiento interno para la elevación de asuntos para su consideración y su adopción. La aprobación del Reglamento requerirá el voto favorable de, al menos, seis de los miembros del Consejo.

## CAPÍTULO IV

## Régimen de actuación y potestades

**Artículo 27.** *Facultades de inspección.*

1. El personal funcionario de carrera de la Comisión Nacional de los Mercados y la Competencia, debidamente autorizado por el director correspondiente, tendrá la condición de agente de la autoridad y podrá realizar cuantas inspecciones sean necesarias en las empresas y asociaciones de empresas para la debida aplicación de esta Ley.

2. El personal habilitado a tal fin tendrá las siguientes facultades de inspección:

a) Acceder a cualquier local, instalación, terreno y medio de transporte de las empresas y asociaciones de empresas y al domicilio particular de los empresarios, administradores y otros miembros del personal de las empresas. Asimismo podrán controlar los elementos afectos a los servicios o actividades que los operadores o quienes realicen las actividades a las que se refiere esta Ley, de las redes que instalen o exploten y de cuantos documentos están obligados a poseer o conservar.

b) Verificar los libros, registros y otros documentos relativos a la actividad de que se trate, cualquiera que sea su soporte material, incluidos los programas informáticos y los archivos magnéticos, ópticos o de cualquier otra clase.

c) Hacer u obtener copias o extractos, en cualquier formato, de dichos libros o documentos.

d) Retener por un plazo máximo de diez días los libros o documentos mencionados en la letra b).

e) Precintar todos los locales, libros o documentos y demás bienes de la empresa durante el tiempo y en la medida en que sea necesario para la inspección.

f) Solicitar a cualquier representante o miembro del personal de la empresa o de la asociación de empresas explicaciones sobre hechos o documentos relacionados con el objeto y la finalidad de la inspección y guardar constancia de sus respuestas.

El ejercicio de las facultades descritas en las letras a) y e) requerirá el previo consentimiento expreso del afectado o, en su defecto, la correspondiente autorización judicial.

3. Las empresas y asociaciones de empresas están obligadas a someterse a las inspecciones que el órgano competente haya autorizado.

4. Si la empresa o asociación de empresas se opusieran a una inspección o existiese el riesgo de tal oposición, el órgano competente de la Comisión deberá solicitar la correspondiente autorización judicial, cuando la misma implique restricción de derechos fundamentales, al Juzgado de lo Contencioso-Administrativo, que resolverá en el plazo máximo de 48 horas. Las autoridades públicas prestarán la protección y el auxilio necesario al personal de la Comisión Nacional de los Mercados y la Competencia para el ejercicio de las funciones de inspección.

5. El personal funcionario de carrera encargado de la inspección levantará acta de sus actuaciones. Las actas extendidas tendrán naturaleza de documentos públicos y harán prueba, salvo que se acredite lo contrario, de los hechos que motiven su formalización.

6. Los datos e informaciones obtenidos sólo podrán ser utilizados por la Comisión Nacional de los Mercados y la Competencia para las finalidades previstas en esta Ley y en la Ley 15/2007, de 3 de julio.

**Artículo 28.** *Requerimientos de información, deber de secreto y acceso a los registros estatales.*

1. Toda persona física o jurídica y los órganos y organismos de cualquier Administración Pública quedan sujetos al deber de colaboración con la Comisión Nacional de los Mercados y la Competencia en el ejercicio de la protección de la libre competencia y están obligados a proporcionar, a requerimiento de ésta y en plazo, toda clase de datos e informaciones de que dispongan y que puedan resultar necesarias para el desarrollo de las funciones de dicha Comisión.

Los requerimientos de información habrán de estar motivados y ser proporcionados al fin perseguido. En los requerimientos que dicte al efecto, se expondrá de forma detallada y concreta el contenido de la información que se vaya a solicitar, especificando de manera justificada la función para cuyo desarrollo es precisa tal información y el uso que pretende hacerse de la misma.

2. Los datos e informaciones obtenidos por la Comisión Nacional de los Mercados y la Competencia en el desempeño de sus funciones, con la excepción de los previstos por las letras c), d), e) y f) del apartado 1 del artículo 5 de esta Ley, que tengan carácter confidencial por tratarse de materias protegidas por el secreto comercial, industrial o estadístico, sólo podrán ser cedidos al Ministerio competente, a las Comunidades Autónomas, a la Comisión

Europea y a las autoridades de otros Estados miembros de la Unión Europea en el ámbito de sus competencias, así como a los tribunales en los procesos judiciales correspondientes.

Quien tenga conocimiento de estos datos estará obligado a guardar sigilo respecto de los mismos. Sin perjuicio de las responsabilidades penales y civiles que pudieran corresponder, la violación del deber de sigilo se considerará falta disciplinaria muy grave.

3. La Comisión Nacional de los Mercados y la Competencia tendrá acceso a los registros previstos en la legislación estatal reguladora de los sectores incluidos en el ámbito de aplicación de esta Ley. Asimismo, la Administración General del Estado tendrá acceso a las bases de datos que obren en poder de la Comisión Nacional de los Mercados y la Competencia.

A estos efectos, se realizarán los desarrollos informáticos oportunos con el fin de facilitar el acceso electrónico a que se refiere el párrafo anterior, de forma que se puedan realizar consultas sobre información contenidas en las bases de datos y registros en condiciones que mantengan la seguridad, confidencialidad e integridad de la información.

**Artículo 29.** *Potestad sancionadora.*

1. La Comisión Nacional de los Mercados y la Competencia tendrá facultades de inspección en el ejercicio de sus competencias. Asimismo, podrá imponer sanciones de acuerdo con lo previsto en el Capítulo II del Título IV de la Ley 15/2007, de 3 de julio, en el Título VI de la Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual, en el Título X de la Ley 24/2013, de 26 de diciembre, del Sector Eléctrico, en el Título VI de la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos, en el Título VIII de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, en el título VII de la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal y en el Título VII de la Ley 38/2015, de 29 de septiembre, del sector ferroviario.

2. Para el ejercicio de la potestad sancionadora, se garantizará la debida separación funcional entre la fase instructora, que corresponderá al personal de la dirección correspondiente en virtud de la materia, y la resolutoria, que corresponderá al Consejo.

3. El procedimiento para el ejercicio de la potestad sancionadora se regirá por lo establecido en esta Ley en las leyes mencionadas en el apartado 1, así como, en lo no previsto en las normas anteriores, por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en su normativa de desarrollo. En concreto, el procedimiento sancionador en materia de defensa de la competencia se regirá por las disposiciones específicas previstas en la Ley 15/2007, de 3 de julio.

4. La resolución del procedimiento pondrá fin a la vía administrativa y contra ella podrá interponerse recurso contencioso-administrativo.

5. La recaudación de las multas corresponderá a las Delegaciones de Economía y Hacienda en período voluntario y a la Agencia Estatal de Administración Tributaria en período ejecutivo, conforme a lo establecido en el Reglamento General de Recaudación aprobado por el Real Decreto 939/2005, de 29 de julio.

**Artículo 30.** *Circulares, circulares informativas y comunicaciones de la Comisión Nacional de los Mercados y la Competencia.*

1. La Comisión Nacional de los Mercados y la Competencia podrá dictar las disposiciones de desarrollo y ejecución de las leyes, reales decretos y órdenes ministeriales que se aprueben en relación con los sectores sometidos a su supervisión cuando le habiliten expresamente para ello. Estas disposiciones adoptarán la forma de circulares de la Comisión Nacional de los Mercados y la Competencia.

Las circulares tendrán carácter vinculante para los sujetos afectados por su ámbito de aplicación, una vez publicadas en el «Boletín Oficial del Estado».

En el procedimiento de elaboración de las circulares se dará audiencia a los titulares de derechos e intereses legítimos que resulten afectados por las mismas, directamente o a través de las organizaciones y asociaciones reconocidas por la ley que los agrupen o los representen y cuyos fines guarden relación directa con el objeto de la circular, y se fomentará en general la participación de los ciudadanos.

2. Sin perjuicio de lo establecido en el apartado anterior, la Comisión Nacional de los Mercados y la Competencia podrá efectuar requerimientos de información periódica y dirigidos a la generalidad de los sujetos afectados. Estos requerimientos adoptarán la forma de circulares informativas.

Las circulares informativas habrán de ser motivadas y proporcionadas al fin perseguido y respetarán la garantía de confidencialidad de la información aportada, de conformidad con lo establecido en el artículo 28 de esta Ley.

En ellas se expondrá de forma detallada y concreta el contenido de la información que se vaya a solicitar, especificando de manera justificada la función para cuyo desarrollo es precisa tal información y el uso que se hará de la misma.

3. La Comisión Nacional de los Mercados y la Competencia podrá dictar comunicaciones que aclaren los principios que guían su actuación.

**Artículo 31.** *Régimen jurídico del personal.*

1. El personal que preste servicios en la Comisión Nacional de los Mercados y la Competencia será funcionario o laboral, en los términos establecidos en la Administración General del Estado, de acuerdo con lo que se disponga reglamentariamente y de conformidad con lo dispuesto en el apartado 4 de este artículo.

2. El personal funcionario se regirá por las normas reguladoras de la función pública aplicables al personal funcionario de la Administración General del Estado.

La provisión de puestos de trabajo del personal funcionario se llevará a cabo de conformidad con los procedimientos de provisión establecidos en la normativa sobre función pública aplicable al personal funcionario de la Administración General del Estado.

3. El personal laboral se regirá por el Texto Refundido del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 1/1995, de 24 de marzo, la normativa convencional aplicable, y por los preceptos de la Ley 7/2007, de 12 de abril, que expresamente le resulten de aplicación.

La selección del personal laboral se llevará a cabo, en ejecución de la oferta de empleo público de la Administración General del Estado, mediante convocatoria pública, con sujeción a los principios de igualdad, mérito y capacidad, así como de acceso al empleo público de las personas con discapacidad.

4. La Comisión Nacional de los Mercados y la Competencia contará con una relación de puestos de trabajo que deberá ser aprobada por el Ministerio de Hacienda y Administraciones Públicas, en la que constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas.

5. Sin perjuicio de lo dispuesto en el artículo 25 de esta Ley, se determinarán en el Estatuto Orgánico los puestos de trabajo que por su especial responsabilidad, competencia técnica o relevancia de sus tareas, tienen naturaleza directiva. El personal directivo será funcionario de carrera del subgrupo A1 y, con carácter excepcional, se podrán cubrir dichos puestos en régimen laboral mediante contratos de alta dirección, siempre que no tengan atribuido el ejercicio de potestades o funciones públicas incluidas en el ámbito del artículo 9.2 de la Ley 7/2007, de 12 de abril. La cobertura de estos puestos se realizará en los términos previstos en el artículo 26.3 de esta Ley.

A los contratos de alta dirección les será de aplicación lo dispuesto en la Disposición adicional octava de la Ley 3/2012, de 6 de julio, de medidas urgentes para la reforma del mercado laboral, y en el Real Decreto 451/2012, de 5 de marzo, por el que se regula el régimen retributivo de los máximos responsables y directivos del sector público empresarial.

6. La determinación y modificación de las condiciones retributivas, tanto del personal directivo, como del resto del personal, requerirá el informe previo y favorable del Ministerio de Hacienda y Administraciones Públicas. Respecto al personal directivo se estará a lo dispuesto en el Real Decreto 451/2012, de 5 de marzo, y a las demás normas, en especial las de presupuestos, que sean aplicables.

Asimismo, el Ministerio de Hacienda y Administraciones Públicas efectuará con la periodicidad adecuada controles específicos sobre la evolución de los gastos de personal y

de la gestión de sus recursos humanos, de conformidad con los criterios que a tal efecto haya establecido.

**Artículo 32.** *Régimen de contratación.*

Los contratos que celebre la Comisión Nacional de los Mercados y la Competencia se ajustarán a lo dispuesto en la legislación sobre contratación del sector público, siendo su órgano de contratación el Presidente de la misma.

**Artículo 33.** *Régimen económico-financiero y patrimonial.*

1. La Comisión Nacional de los Mercados y la Competencia tendrá patrimonio propio e independiente del patrimonio de la Administración General del Estado.
2. La Comisión Nacional de los Mercados y la Competencia contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.
b) Los bienes y derechos que constituyan su patrimonio así como los productos y rentas del mismo.
c) Cualesquiera otros que legalmente puedan serle atribuidos.

3. El control económico y financiero de la Comisión Nacional de los Mercados y la Competencia se efectuará con arreglo a lo dispuesto en la Ley 47/2003, de 26 de noviembre, General Presupuestaria, y en la Ley Orgánica 2/1982, de 12 de mayo, del Tribunal de Cuentas.

**Artículo 34.** *Presupuesto, régimen de contabilidad y control económico y financiero.*

1. La Comisión Nacional de los Mercados y la Competencia elaborará y aprobará anualmente un anteproyecto de presupuesto, cuyos créditos tendrán carácter limitativo, y lo remitirá al Ministerio de Hacienda y Administraciones Públicas a través del Ministerio de Economía y Competitividad para su posterior tramitación de acuerdo con lo previsto en la Ley 47/2003, de 26 de noviembre.
2. El régimen de variaciones y de vinculación de los créditos de dicho presupuesto será el que se establezca en el Estatuto Orgánico de la Comisión Nacional de los Mercados y la Competencia.
3. Corresponde al Presidente de la Comisión Nacional de los Mercados y la Competencia aprobar los gastos y ordenar los pagos y efectuar la rendición de cuentas del organismo de conformidad con lo dispuesto en la Ley 47/2003, de 26 de noviembre.
4. La Comisión Nacional de los Mercados y la Competencia formulará y rendirá sus cuentas de acuerdo con la Ley 47/2003, de 26 de noviembre, y las normas y principios de contabilidad recogidos en el Plan General de Contabilidad Pública y sus normas de desarrollo. La Comisión Nacional de los Mercados y la Competencia dispondrá de un sistema de contabilidad analítica que proporcione información de costes sobre su actividad que sea suficiente para una correcta y eficiente adopción de decisiones.
5. Sin perjuicio de las competencias atribuidas al Tribunal de Cuentas por su Ley Orgánica, la gestión económico financiera de la Comisión Nacional de los Mercados y la Competencia estará sometida al control de la Intervención General de la Administración del Estado en los términos que establece la Ley 47/2003, de 26 de noviembre. El control financiero permanente se realizará por la Intervención Delegada en la Comisión Nacional bajo la dependencia funcional de la Intervención General de la Administración del Estado.

**Artículo 35.** *Asistencia jurídica.*

La asistencia jurídica, consistente en el asesoramiento, representación y defensa en juicio de la Comisión Nacional de los Mercados y la Competencia, corresponde al Servicio Jurídico del Estado cuyo centro directivo superior es la Abogacía General del Estado-Dirección del Servicio Jurídico, mediante la formalización del oportuno convenio en los términos previstos en la Ley 52/1997, de 27 de noviembre, de Asistencia Jurídica del Estado e Instituciones Públicas y su normativa de desarrollo.

**Artículo 36.** *Recursos contra los actos, las decisiones y las resoluciones de la Comisión Nacional de los Mercados y la Competencia.*

1. Los actos y decisiones de los órganos de la Comisión distintos del Presidente y del Consejo podrán ser objeto de recurso administrativo conforme a lo dispuesto en la Ley 30/1992, de 26 de noviembre.

No obstante, respecto a los actos dictados en aplicación de la Ley 15/2007, de 3 de julio, únicamente podrán ser objeto de recurso aquéllos a los que hace referencia el artículo 47 de dicha Ley.

2. Los actos y resoluciones del Presidente y del Consejo, en pleno y en salas, de la Comisión Nacional de los Mercados y la Competencia dictados en el ejercicio de sus funciones públicas pondrán fin a la vía administrativa y no serán susceptibles de recurso de reposición, siendo únicamente recurribles ante la jurisdicción contencioso-administrativa.

## CAPÍTULO V

## Transparencia y responsabilidad

**Artículo 37.** *Publicidad de las actuaciones.*

1. La Comisión Nacional de los Mercados y la Competencia hará públicas todas las disposiciones, resoluciones, acuerdos e informes que se dicten en aplicación de las leyes que las regulan, una vez notificados a los interesados, tras resolver en su caso sobre los aspectos confidenciales de su contenido y previa disociación de los datos de carácter personal a los que se refiere el artículo 3.a) de la Ley Orgánica 15/1999, de 13 de diciembre, salvo en lo que se refiere al nombre de los infractores. En particular, se difundirán:

a) La organización y funciones de la Comisión y de sus órganos, incluyendo los currículum vítae de los miembros del Consejo y del personal directivo.

b) La relación de los acuerdos adoptados en las reuniones del Consejo.

c) Los informes en que se basan las decisiones del Consejo.

d) La memoria anual de actividades que incluya las cuentas anuales y su comparación con las cuentas anuales de los dos años anteriores, la situación organizativa y la información relativa al personal, la composición del Consejo indicando los cambios que se puedan haber producido respecto al año anterior, y las actividades realizadas por la Comisión, con los objetivos perseguidos y los resultados alcanzados, que se enviará a la Comisión correspondiente del Congreso de los Diputados y a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital.

e) Los informes económicos sectoriales, de carácter anual, en los que se analizará la situación competitiva del sector, la actuación del sector público y las perspectivas de evolución del sector, sin perjuicio de los informes que puedan elaborar los departamentos ministeriales. El informe se enviará en todo caso a la Comisión correspondiente del Congreso de los Diputados y a los titulares del Ministerio competente en el sector de que se trate y del Ministerio de Economía y Competitividad y en su caso, al titular del Ministerio de Sanidad, Servicios Sociales e Igualdad, en la parte relativa a las reclamaciones de los usuarios finales.

f) Otros informes elaborados sobre la estructura competitiva de mercados o sectores productivos, sin perjuicio de su remisión al titular del Ministerio de Economía y Competitividad.

g) El plan de actuación de la Comisión para el año siguiente, incluyendo las líneas básicas de su actuación en ese año, con los objetivos y prioridades correspondientes. Este plan de actuaciones se enviará también a la Comisión correspondiente del Congreso de los Diputados y al titular del Ministerio de Economía y Competitividad.

h) Los informes elaborados sobre proyectos normativos o actuaciones del sector público.

i) Las reuniones de los miembros de la Comisión con empresas del sector, siempre que su publicidad no afecte al cumplimiento de los fines que tiene encomendada la Comisión Nacional de los Mercados y la Competencia.

j) Las resoluciones que pongan fin a los procedimientos.

k) Las resoluciones que acuerden la imposición de medidas cautelares.

l) La iniciación de un expediente de control de concentraciones.
m) La incoación de expedientes sancionadores.
n) La realización de inspecciones de acuerdo con la Ley 15/2007, de 3 de julio.

2. Las disposiciones, resoluciones, acuerdos, informes y la memoria anual de actividades y el plan de actuación se harán públicos por medios electrónicos.
3. Cada tres años, la Comisión Nacional de los Mercados y la Competencia presentará una evaluación de sus planes de actuación y los resultados obtenidos para poder valorar su impacto en el sector y el grado de cumplimiento de las resoluciones dictadas. Estas evaluaciones se enviarán también a la Comisión correspondiente del Congreso de los Diputados y al titular del Ministerio de Economía y Competitividad.

**Artículo 38.** *Medidas para mejorar la eficiencia, eficacia y calidad de los procedimientos de supervisión.*

1. Sin perjuicio de las competencias atribuidas a otros órganos por el Capítulo IV de esta Ley en materia de control económico y financiero, la Comisión dispondrá de un órgano de control interno cuya dependencia funcional y capacidad de informe se regirá por los principios de imparcialidad, objetividad y evitar la producción de conflictos de intereses.
2. La Comisión elaborará anualmente una memoria sobre su función supervisora que incluirá un informe del órgano de control interno sobre la adecuación de las decisiones adoptadas por la Comisión a la normativa procedimental aplicable. Esta memoria deberá ser aprobada por el Consejo y remitida a las Cortes Generales y al Ministerio de Economía y Competitividad.

**Artículo 39.** *Control parlamentario.*

1. El Presidente de la Comisión Nacional de los Mercados y la Competencia deberá comparecer con periodicidad al menos anual ante la Comisión correspondiente del Congreso de los Diputados para exponer las líneas básicas de su actuación y sus planes y prioridades para el futuro. Junto con el Presidente, podrán comparecer, a petición de la Cámara, uno o varios miembros del Consejo.
2. Las comparecencias anuales estarán basadas en la memoria anual de actividades y el plan de actuación.
3. Sin perjuicio de su comparecencia anual, el Presidente comparecerá ante la Comisión correspondiente del Congreso o del Senado, a petición de las mismas en los términos establecidos en sus respectivos Reglamentos.
4. Cada tres años el Presidente comparecerá de forma especial para debatir la evaluación del plan de actuación y el resultado obtenido por la Comisión Nacional de los Mercados y la Competencia.

**Disposición adicional primera.** *Constitución y ejercicio efectivo de las funciones de la Comisión Nacional de los Mercados y la Competencia.*

1. Inmediatamente después de la aprobación del Estatuto Orgánico, el Ministro de Economía y Competitividad propondrá al Gobierno el nombramiento de los miembros del Consejo, quienes comparecerán ante el Congreso, que tendrá un mes para vetarlos en los términos del artículo 15 de esta Ley.
2. En el plazo de 20 días desde la publicación del real decreto de nombramiento de los miembros del Consejo, se procederá a la constitución de la Comisión Nacional de los Mercados y la Competencia, a través de la constitución del Consejo. Una vez constituido, el Consejo procederá a nombrar al Secretario.
3. Constituida la Comisión, el Consejo contará con el plazo de un mes para llevar a cabo las siguientes acciones:

a) Nombramiento del personal directivo, de acuerdo con lo establecido en el artículo 26.3 de esta Ley.
b) Elaboración del Reglamento de funcionamiento interno.
c) Integración de medios personales y materiales que correspondan a la Comisión Nacional de los Mercados y la Competencia.

4. La puesta en funcionamiento de la Comisión Nacional de los Mercados y la Competencia, que implicará el ejercicio efectivo por parte de sus órganos de las funciones que tienen atribuidas, se iniciará en la fecha que al efecto se determine por orden del Ministro de Economía y Competitividad y, en todo caso, en el plazo de cuatro meses desde la entrada en vigor de esta Ley. En esta fecha se tendrá que haber producido la transferencia del personal y de los medios presupuestarios suficientes para el desempeño de las funciones recogidas en esta Ley.

**Disposición adicional segunda.** *Extinción de organismos.*

1. La constitución de la Comisión Nacional de los Mercados y la Competencia implicará la extinción de la Comisión Nacional de la Competencia, la Comisión Nacional de Energía, la Comisión del Mercado de las Telecomunicaciones, la Comisión Nacional del Sector Postal, el Comité de Regulación Ferroviaria, la Comisión Nacional del Juego, la Comisión de Regulación Económica Aeroportuaria y el Consejo Estatal de Medios Audiovisuales.

2. Sin perjuicio de lo establecido en esta Ley, las referencias que la legislación vigente contiene a la Comisión Nacional de la Competencia, la Comisión Nacional de Energía, la Comisión del Mercado de las Telecomunicaciones, la Comisión Nacional del Sector Postal, el Consejo Estatal de Medios Audiovisuales, la Comisión de Regulación Económica Aeroportuaria y el Comité de Regulación Ferroviaria se entenderán realizadas a la Comisión Nacional de los Mercados y la Competencia o al ministerio correspondiente según la función de que se trate.

Las referencias que la Ley 15/2007, de 3 de julio, contiene a la Dirección de Investigación de la Comisión Nacional de Competencia se entenderán realizadas a la Dirección de Competencia de la Comisión Nacional de los Mercados y la Competencia.

Las menciones a la Autoridad Estatal de Supervisión regulada en el Título VI de la Ley 21/2003, de 7 de julio, que se contienen en dicha Ley o en cualquier otra disposición, deberán entenderse realizadas a la Comisión Nacional de los Mercados y la Competencia.

3. Las referencias contenidas en cualquier norma del ordenamiento jurídico a la Comisión Nacional del Juego se entenderán realizadas a la Dirección General de Ordenación del Juego del Ministerio de Consumo que la sustituye y asume sus competencias, en los términos previstos en la disposición adicional décima.

4. Sin perjuicio de lo previsto en el apartado 6, la Comisión Nacional de los Mercados y la Competencia asumirá los medios materiales, incluyendo, en particular, sistemas y aplicaciones informáticas de los organismos extinguidos a los que se refiere el apartado 1, que resulten necesarios para el ejercicio de sus funciones, correspondiendo el resto a los ministerios que asuman las funciones atribuidas en las Disposiciones adicionales séptima, octava, novena, décima, undécima y duodécima.

5. Los Ministerios de Hacienda y Administraciones Públicas y de Economía y Competitividad determinarán los saldos de tesorería y los activos financieros de los organismos que se extinguen que deban incorporarse a la Comisión Nacional de los Mercados y la Competencia.

6. Los bienes inmuebles y derechos reales de titularidad de los organismos reguladores extinguidos que resulten innecesarios para el ejercicio de las funciones de la Comisión Nacional de los Mercados y la Competencia se incorporarán al patrimonio de la Administración General del Estado.

**Disposición adicional tercera.** *Régimen especial de incompatibilidad e indemnización del Presidente, Vicepresidente y consejeros de los organismos que se extinguen.*

1. Durante los dos años posteriores a su cese, el Presidente, el Vicepresidente y los consejeros de los organismos que se extinguen, no podrán ejercer actividad profesional privada alguna relacionada con el sector regulado, tanto en empresas del sector como para empresas del sector, en el caso de los Organismos Reguladores. En el caso de la Comisión Nacional de la Competencia, al cesar en su cargo, y durante los dos años posteriores, el Presidente y los consejeros no podrán ejercer actividad profesional privada alguna relacionada con la actividad de la Comisión.

2. En virtud de esta limitación, el Presidente, el Vicepresidente y los consejeros de los organismos que se extinguen, al cesar en su cargo, tendrán derecho a percibir, a partir del

mes siguiente a aquel en que se produzca su cese y durante un plazo igual al que hubieran desempeñado el cargo, con el límite máximo de dos años, una compensación económica mensual igual a la doceava parte del ochenta por ciento del total de retribuciones asignadas al cargo respectivo en el presupuesto en vigor durante el plazo indicado.

No habrá lugar a la percepción de dicha compensación en caso de desempeño, de forma remunerada, de cualquier puesto de trabajo, cargo o actividad en el sector público o privado en los términos previstos en el artículo 1 del Real Decreto-Ley 20/2012, de 13 de julio, de medidas para garantizar la estabilidad presupuestaria y de fomento de la competitividad.

**Disposición adicional cuarta.** *Asignación de medios a la Administración General del Estado.*

1. En el plazo previsto en la Disposición adicional primera de esta Ley para la puesta en funcionamiento de la Comisión, el Gobierno aprobará las modificaciones necesarias en los reales decretos de desarrollo de la estructura orgánica básica de los Ministerios afectados.

2. La entrada en vigor de las modificaciones de los reales decretos de estructura a que hace referencia esta Disposición, no se producirá hasta que los presupuestos de los ministerios no se adecúen a la nueva distribución competencial, de acuerdo con lo establecido en la Disposición transitoria cuarta.

**Disposición adicional quinta.** *Atribución de competencias a la Comisión Nacional de los Mercados y la Competencia.*

Las competencias que las normas vigentes atribuyen a los organismos que se extingan cuando se constituya la Comisión Nacional de los Mercados y la Competencia y que esta Ley no haya atribuido expresamente a los departamentos ministeriales competentes de la Administración General del Estado serán ejercidas por la Comisión Nacional de los Mercados y la Competencia.

**Disposición adicional sexta.** *Integración del personal de los organismos públicos que se extinguen en la Comisión Nacional de los Mercados y la Competencia.*

1. El personal funcionario que presta servicios en los organismos que se extinguirán de acuerdo con lo establecido en la Disposición adicional segunda, se integrará en la Comisión Nacional de los Mercados y la Competencia, o bien en la Administración General del Estado.

La integración se llevará a cabo, en ambos supuestos, de acuerdo con los procedimientos de movilidad establecidos en la legislación de función pública aplicable al personal funcionario de la Administración General del Estado.

El personal funcionario que se integre en la Comisión Nacional de los Mercados y la Competencia, lo hará en la situación de servicio activo en su correspondiente Cuerpo o Escala, con los mismos derechos y obligaciones que hasta ese momento tuviera reconocidos.

Igual situación administrativa y garantías tendrán los funcionarios que pasen a prestar servicios en la Administración General del Estado como consecuencia de las competencias que ésta asuma de los extintos organismos.

2. El personal laboral de los organismos que ahora se extinguen, se integrará en la Comisión Nacional de los Mercados y la Competencia en los términos previstos en el artículo 44 del Texto Refundido del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 1/1995, de 24 de marzo, con respeto a los derechos y obligaciones laborales que viniera ostentando hasta ese momento.

Para la integración de este personal laboral, se atenderá necesariamente a las funciones efectivas que vinieran desempeñando en el organismo extinguido.

Excepcionalmente, el personal laboral podrá integrarse en los departamentos ministeriales, en los mismos términos previstos en el párrafo anterior, cuando como consecuencia de las funciones que por esta Ley se atribuyen a los departamentos ministeriales se haga necesaria su integración, sin que en ningún caso puedan producirse incrementos retributivos con relación a la situación existente en los organismos de procedencia. Cuando queden vacantes los puestos de trabajo que se integren en la estructura orgánica de dichos departamentos por fallecimiento, jubilación o cualquier otra

causa legal, y siempre que esta no implique derecho al reingreso en el servicio activo, se amortizarán, dándose de alta como plazas de personal funcionario para garantizar la continuidad en la prestación de las citadas funciones, siempre y cuando ello resulte necesario de conformidad con lo establecido en el artículo 9 de la Ley 7/2007, de 12 de abril. La reasignación de efectivos, amortización y, en su caso, creación de puestos de trabajo tendrá lugar en los términos y con el alcance que se determine por el órgano competente.

**Disposición adicional séptima.** *Funciones que asume el Ministerio de Industria, Energía y Turismo en materia audiovisual.*

En materia audiovisual de ámbito estatal, el Ministerio de Industria, Energía y Turismo ejercerá, adicionalmente a las que ya tiene encomendadas, las siguientes funciones:

a) Recibir las comunicaciones de inicio de actividad de los prestadores del servicio de comunicación audiovisual.

b) Llevar el Registro estatal de prestadores de servicios de comunicación audiovisual.

c) Decidir sobre cualquier cuestión o incidente que afecte al ejercicio de los títulos habilitantes de servicios de comunicación audiovisual, tales como su duración, renovación, modificación, celebración de negocios jurídicos o extinción.

d) Verificar las condiciones de los artículos 36 y 37 de la Ley 7/2010, de 31 de marzo, en materia de limitación de adquisición de participaciones entre operadores del servicio de comunicación audiovisual.

e) Certificar la emisión en cadena por parte de los prestadores del servicio de comunicación audiovisual radiofónica que así lo comunicasen, e instar su inscripción, cuando proceda, en el Registro estatal de prestadores de servicios de comunicación audiovisual.

**Disposición adicional octava.** *Funciones que asume el Ministerio de Industria, Energía y Turismo en materia de energía.*

El Ministerio de Industria, Energía y Turismo asumirá las siguientes funciones:

1. En el sector eléctrico:

a) Inspeccionar, dentro de su ámbito de competencias, el cumplimiento de las condiciones técnicas de las instalaciones, el cumplimiento de los requisitos establecidos en las autorizaciones, la correcta y efectiva utilización del carbón autóctono en las centrales eléctricas con derecho al cobro de la prima al consumo de carbón autóctono, las condiciones económicas y actuaciones de los sujetos en cuanto puedan afectar a la aplicación de las tarifas, precios y criterios de remuneración de las actividades energéticas, la disponibilidad efectiva de las instalaciones de generación en el régimen ordinario, la correcta facturación y condiciones de venta de las empresas distribuidoras y comercializadoras a consumidores y clientes cualificados, la continuidad del suministro de energía eléctrica, la calidad del servicio, así como la efectiva separación de estas actividades cuando sea exigida.

b) Acordar la iniciación de los expedientes sancionadores y realizar la instrucción de los mismos, cuando sean de la competencia de la Administración General del Estado por no corresponder la incoación e instrucción de los mismos a la Comisión Nacional de los Mercados y la Competencia, e informar, cuando sea requerida para ello, aquellos expedientes sancionadores iniciados por las distintas Administraciones Públicas.

c) Informar, atender y tramitar, en coordinación con las administraciones competentes, a través de protocolos de actuación, las reclamaciones planteadas por los consumidores de energía eléctrica y tener a disposición de los mismos toda la información necesaria relativa a sus derechos, a la legislación en vigor y a las vías de solución de conflictos de que disponen en caso de litigios.

El Ministerio de Industria, Energía y Turismo informará, al menos semestralmente, a la Comisión Nacional de los Mercados y la Competencia de las actuaciones realizadas, incluyendo información sobre el número de reclamaciones informadas, atendidas y tramitadas con el fin de facilitar las labores de supervisión del funcionamiento de los mercados minoristas por parte de este organismo.

d) Realizar la liquidación de los costes de transporte y distribución de energía eléctrica, de los costes permanentes del sistema y de aquellos otros costes que se establezcan para el

conjunto del sistema cuando su liquidación le sea expresamente encomendada y enviar a la Comisión Nacional de los Mercados y la Competencia toda la información necesaria para la elaboración de las metodologías de peajes.

e) Supervisar la actividad de la Oficina de Cambios de Suministrador.

2. En el sector de hidrocarburos:

a) Inspeccionar dentro de su ámbito de competencias, el cumplimiento de las condiciones técnicas de las instalaciones, el cumplimiento de los requisitos establecidos en las autorizaciones, las condiciones económicas y actuaciones de los sujetos en cuanto puedan afectar a la aplicación de las tarifas, precios y criterios de remuneración de las actividades de hidrocarburos, la disponibilidad efectiva de las instalaciones gasistas, la correcta facturación y condiciones de venta a los consumidores de las empresas distribuidoras, en lo que se refiere al acceso a las redes, y comercializadoras, la continuidad del suministro de gas natural, la calidad del servicio, así como la efectiva separación de estas actividades cuando sea exigida.

b) Acordar, en el ámbito de aplicación de la Ley 34/1998, de 7 de octubre, la iniciación de los expedientes sancionadores y realizar la instrucción de los mismos, cuando sean de la competencia de la Administración General del Estado e informar, cuando sea requerida para ello, aquellos expedientes sancionadores iniciados por las distintas Administraciones Públicas, sin perjuicio de las competencias atribuidas a la Corporación de Reservas Estratégicas de Productos Petrolíferos en el artículo 52.4 de la citada Ley ni de las competencias exclusivas de otros órganos de las Administraciones Públicas.

c) Realizar las liquidaciones correspondientes a los ingresos obtenidos por peajes y cánones relativos al uso de las instalaciones de la Red Básica, transporte secundario y distribución a que hace referencia el artículo 96 de la Ley 34/1998, de 7 de octubre, y comunicarla a los interesados.

d) Informar, atender y tramitar, en coordinación con las Administraciones competentes, a través de protocolos de actuación, las reclamaciones planteadas por los consumidores de gas natural, y tener a disposición de los mismos toda la información necesaria relativa a sus derechos, a la legislación en vigor y a las vías de solución de conflictos de que disponen en caso de litigios.

El Ministerio de Industria, Energía y Turismo informará, al menos semestralmente, a la Comisión Nacional de los Mercados y la Competencia de las actuaciones realizadas, incluyendo información sobre el número de reclamaciones informadas, atendidas y tramitadas con el fin de facilitar las labores de supervisión del funcionamiento de los mercados minoristas por parte de este organismo.

e) Expedir los certificados y gestionar el mecanismo de certificación de consumo y venta de biocarburantes.

f) Supervisar la actividad de la Oficina de Cambios de Suministrador.

g) Las competencias que la normativa vigente atribuye a la Comisión Nacional de la Energía en materia de hidrocarburos líquidos.

3. En el sector eléctrico y de hidrocarburos: conocer la toma de participaciones en el sector energético.

**Disposición adicional novena.** *Toma de participaciones en el sector energético.*

1. El Ministerio de Industria, Energía y Turismo conocerá de las siguientes operaciones:

a) Toma de participaciones en sociedades o por parte de sociedades que desarrollen actividades que tengan la consideración de reguladas, consistan en la operación del mercado de energía eléctrica o se trate de actividades en territorios insulares o extra peninsulares conforme a lo dispuesto en la Ley 54/1997, de 27 de noviembre, del Sector Eléctrico.

b) Toma de participaciones en sociedades o por parte de sociedades que desarrollen actividades que tengan la consideración de reguladas, consistan en la gestión técnica del sistema gasista conforme a lo dispuesto en la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos, o desarrollen actividades en el sector de hidrocarburos tales como refino de petróleo, transporte por oleoductos y almacenamiento de productos petrolíferos.

c) Toma de participaciones en sociedades o por parte de sociedades que sean titulares de los activos precisos para desarrollar las actividades recogidas en las letras a) y b), o bien de activos del sector de la energía de carácter estratégico incluidos en el Catálogo Nacional de infraestructuras críticas de acuerdo a lo dispuesto en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y su normativa de desarrollo.

En todo caso, se considerarán activos estratégicos las centrales térmicas nucleares y las centrales térmicas de carbón de especial relevancia en el consumo de carbón de producción nacional, así como las refinerías de petróleo, los oleoductos y los almacenamientos de productos petrolíferos.

d) Adquisición de los activos mencionados en la letra c) anterior.

2. Las sociedades que realicen actividades incluidas en las letras a) y b) del apartado 1 anterior, deberán comunicar a la Secretaría de Estado de Energía del Ministerio para la Transición Ecológica y el Reto Demográfico las adquisiciones realizadas directamente o mediante sociedades que controlen conforme a los criterios establecidos en el artículo 42.1 del Código de Comercio, de participaciones en otras sociedades mercantiles o de activos de cualquier naturaleza que atendiendo a su valor o a otras circunstancias tengan un impacto relevante o influencia significativa en el desarrollo de las actividades de la sociedad que comunica la operación.

En las mismas circunstancias señaladas en el párrafo anterior, se deberán comunicar igualmente las adquisiciones que realicen las sociedades matrices de los grupos de sociedades designadas como gestor de la red de transporte de electricidad y gas natural, así como cualesquiera otras sociedades que formen parte de dichos grupos.

3. Igualmente deberá comunicarse a la Secretaría de Estado de Energía la adquisición de participaciones en un porcentaje de su capital social que conceda una influencia significativa en su gestión, en las sociedades que, directamente o mediante sociedades que controlen conforme a los criterios establecidos en el artículo 42.1 del Código de Comercio, realicen actividades incluidas en el apartado 1 o sean titulares de los activos señalados. De la misma forma, deberá comunicarse la adquisición directa de los activos mencionados en la letra d) del apartado 1.

Además, para la determinación del porcentaje de participación que precisa de comunicación se tomarán en consideración los acuerdos que la sociedad adquirente pueda tener con otros adquirentes o socios para el ejercicio conjunto o coordinado de derechos de voto en la sociedad afectada.

4. Cuando la adquisición señalada en el apartado 3 se realice por entidades de Estados que no sean miembros de la Unión Europea o del Espacio Económico Europeo se estará a lo dispuesto en el apartado 7 de esta Disposición.

5. Asimismo, serán objeto de comunicación por el adquiriente aquellas modificaciones que aisladamente o en su conjunto consideradas puedan suponer un cambio significativo en su participación.

6. Las comunicaciones a las que se refieren los apartados anteriores deberán efectuarse dentro de los 15 días siguientes a la realización de la correspondiente operación, pudiendo indicarse de forma justificada, qué parte de los datos o información aportada se considera de trascendencia comercial o industrial a los efectos de que sea declarada su confidencialidad.

7. Si el Ministro de Industria, Energía y Turismo considerase que existe una amenaza real y suficientemente grave para la garantía de suministro de electricidad, gas e hidrocarburos en el ámbito de las actividades del adquirente, podrá establecer condiciones relativas al ejercicio de la actividad de las sociedades sujetas a las operaciones comunicadas de acuerdo a los apartados 2 y 4 de esta Disposición, así como las obligaciones específicas que se puedan imponer al adquirente para garantizar su cumplimiento.

Estos riesgos se referirán a los siguientes aspectos:

a) La seguridad y calidad del suministro entendidas como la disponibilidad física ininterrumpida de los productos o servicios en el mercado a precios razonables en el corto o largo plazo para todos los usuarios, con independencia de su localización geográfica.

b) La seguridad frente al riesgo de una inversión o de un mantenimiento insuficientes en infraestructuras que no permitan asegurar, de forma continuada, un conjunto mínimo de servicios exigibles para la garantía de suministro. A estos efectos, se tendrá en cuenta el nivel de endeudamiento para garantizar las inversiones, así como el cumplimiento de los compromisos adquiridos al respecto.

c) El incumplimiento de los requisitos de capacidad legal, técnica, económica y financiera del adquiriente o de la empresa adquirida, de acuerdo a lo dispuesto en la normativa específica de aplicación y, en particular, en la Ley 25/1964, de 29 de abril, sobre Energía Nuclear, en la Ley 54/1997, de 27 de noviembre, del Sector Eléctrico, y en la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos, y en sus normas de desarrollo.

A estos efectos, se tomarán en consideración las participaciones que el adquirente tenga o pretenda adquirir en otras sociedades o activos objeto de la presente Disposición.

Las condiciones que se impongan respetarán en todo caso el principio de proporcionalidad y de protección del interés general.

Corresponde al Ministerio de Industria, Energía y Turismo supervisar el cumplimiento de las condiciones que sean impuestas, debiendo las empresas afectadas atender los requerimientos de información que pudieran dictarse a estos efectos.

La resolución deberá adoptarse de forma motivada y notificarse en el plazo máximo de 30 días desde la comunicación, previo informe de la Comisión Nacional de los Mercados y la Competencia. Este informe no tendrá carácter vinculante y habrá de ser evacuado en el plazo de 10 días.

8. Cuando la adquisición de participaciones afecte a los gestores de red de transporte de electricidad o de gas, incluyendo los gestores de red independientes, se estará a lo dispuesto en la Ley 54/1997, de 27 de noviembre, del Sector Eléctrico y en la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos.

**Disposición adicional décima.** *Funciones que asumen la Dirección General de Ordenación del Juego del Ministerio de Consumo y la Agencia Estatal de Administración Tributaria en materia de juego.*

La Dirección General de Ordenación del Juego del Ministerio de Consumo asumirá el objeto, funciones y competencias que la Ley 13/2011, de 27 de mayo, de regulación del juego, atribuye a la extinta Comisión Nacional del Juego, salvo las relacionadas con la gestión y recaudación de las tasas a las que se refiere el artículo 49 de dicha ley, que serán ejercidas por la Agencia Estatal de Administración Tributaria.

**Disposición adicional undécima.** *Funciones que asume el Ministerio de Fomento en relación con el sector postal.*

En materia postal, el Ministerio de Fomento asumirá las siguientes funciones:

1. Informar a los usuarios sobre los operadores postales, las condiciones de acceso, precio, nivel de calidad e indemnizaciones y plazo en el que serán satisfechas y en todo caso, realizar la publicación en el sitio web del Ministerio a que se refiere el artículo 9.2 de la Ley 43/2010, de 30 de diciembre.

2. Conocer de las controversias entre los usuarios y los operadores de los servicios postales en el ámbito del servicio postal universal, siempre y cuando no hayan sido sometidos a las Juntas Arbitrales de Consumo.

3. Conocer de las quejas y denuncias de los usuarios por incumplimiento de las obligaciones por parte de los operadores postales, en relación con la prestación del servicio postal universal, de conformidad con lo establecido el Título II de la Ley 43/2010, de 30 de diciembre, y en su normativa de desarrollo.

El Ministerio de Fomento informará, al menos semestralmente, a la Comisión Nacional de los Mercados y la Competencia de las actuaciones realizadas, incluyendo información sobre el número de reclamaciones informadas, atendidas y tramitadas con el fin de facilitar las labores de supervisión del funcionamiento de los mercados minoristas por parte de este organismo.

4. Ejercer la potestad de inspección y sanción en relación con las funciones mencionadas en los apartados anteriores.

5. Otorgar las autorizaciones singulares y recibir las declaraciones responsables que habilitan para la actividad postal y gestionar el Registro General de empresas prestadoras de servicios postales, de conformidad con lo establecido en el Título IV de la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal, así como en su normativa de desarrollo.

**Disposición adicional duodécima.** *Funciones que asume el Ministerio de la Presidencia en materia audiovisual.*

**(Derogada)**

**Disposición adicional decimotercera.** *Remisión de informes al Instituto Nacional de Consumo.*

Sin perjuicio de las funciones asumidas por los Ministerios de Industria, Energía y Turismo, en materia de energía, y de Fomento, en relación con el sector postal, previstas en la letra c) del apartado 1, y letra d) del apartado 2, de la Disposición adicional octava, y en el apartado 1, de la Disposición adicional undécima, los mencionados Ministerios remitirán al Instituto Nacional del Consumo, dentro del primer trimestre de cada año natural, un informe referido al año anterior en el que se incluya información comprensiva del número de reclamaciones planteadas por los consumidores atendidas, objeto de las mismas, resoluciones estimatorias y desestimatorias adoptadas, sanciones, en su caso, a las que dieron lugar, así como cualquier otro aspecto que se considere relevante.

**Disposición adicional decimocuarta.** *Tasas, prestaciones patrimoniales e ingresos derivados del ejercicio de las funciones previstas en esta Ley.*

1. Los Ministerios y los organismos que desarrollen las funciones previstas en esta Ley, con ocasión de las cuales se produce la exigencia de tasas y prestaciones patrimoniales de carácter público que se recogen en los apartados I.1, I.3, I.4 y I.5 y en el apartado II.1 del Anexo, llevarán a cabo su gestión y recaudación en periodo voluntario, sin perjuicio de lo establecido en la Disposición transitoria novena.

2. La Comisión Nacional de los Mercados y la Competencia llevará a cabo la gestión y recaudación en período voluntario de la tasa prevista en el apartado I.2 y de la prestación patrimonial indicada en el apartado II.2 del Anexo.

3. La recaudación por los derechos a que se refiere esta Disposición adicional, incluida la que correspondiera a los organismos que se extinguen conforme a esta Ley, se ingresará en el Tesoro Público, salvo por lo que respecta al sistema de financiación de la Corporación de Radio Televisión Española y al Fondo de financiación del servicio postal universal, que se regirán por sus respectivas disposiciones.

4. La recaudación en período ejecutivo de los recursos de naturaleza pública a que se refieren los apartados anteriores se efectuará conforme a lo dispuesto en el Reglamento General de Recaudación aprobado por el Real Decreto 939/2005, de 29 de julio.

5. Los recursos a que se refieren los apartados anteriores se regirán, en lo que no se oponga a esta Ley, por la normativa vigente a la entrada en vigor de la misma.

**Disposición adicional decimoquinta.** *Consejos consultivos.*

1. Se crea el Consejo Consultivo de Energía, como órgano de participación y consulta del Ministerio de Industria, Energía y Turismo en las materias competencia de la Secretaría de Estado de Energía.

El Consejo Consultivo de Energía estará presidido por el Secretario de Estado de Energía, o persona en quien delegue, y tendrá entre sus funciones el estudio, deliberación y propuesta en materia de política energética y minas.

Asimismo, conocerá sobre los asuntos que el Gobierno o el Ministro de Industria, Energía y Turismo le sometan.

2. Podrán crearse igualmente consejos consultivos en los sectores de telecomunicaciones, audiovisual, de transportes y postal.

3. Reglamentariamente se determinarán las funciones, la composición, la organización y las reglas de funcionamiento de los consejos consultivos. La constitución y el funcionamiento

de los consejos no supondrán incremento alguno del gasto público y serán atendidos con los medios materiales y de personal existentes en los departamentos respectivos.

4. En todo caso, los consejos consultivos informarán en la elaboración de disposiciones de carácter general y de circulares de la Comisión Nacional de los Mercados y la Competencia. Este informe equivaldrá a la audiencia a los titulares de derechos e intereses legítimos.

**Disposición adicional decimosexta.** *Ejercicio temporal de las funciones de supervisión en materia de tarifas aeroportuarias.*

1. Las funciones establecidas en el artículo 10, letras a) y b), del Real Decreto-Ley 11/2011, de 26 de agosto, por el que se crea la Comisión de Regulación Económica Aeroportuaria y se modifica el régimen jurídico del personal laboral de Aena, pasarán a ser ejercidas por el Comité de Regulación Ferroviaria desde la entrada en vigor de esta Ley, con sujeción a lo dispuesto en los artículos 11 a 13, ambos inclusive, del citado Real Decreto-Ley 11/2011, de 26 de agosto y en el Título VI, Capítulo IV, de la Ley 21/2003, de 7 de julio, de Seguridad Aérea.

2. A partir de la entrada en vigor de esta Ley, el Comité de Regulación Ferroviaria pasará a denominarse Comité de Regulación Ferroviaria y Aeroportuaria.

3. En el ejercicio de las funciones previstas en esta Disposición el Comité de Regulación Ferroviaria y Aeroportuaria actuará con independencia funcional plena, respecto de la organización, de las decisiones financieras, de la estructura legal y de la toma de decisiones, del gestor aeroportuario y de las compañías aéreas, y ejercerá sus funciones de modo imparcial y transparente.

4. En tanto desempeñe las funciones que le atribuye el apartado 1, se entenderán referidas al Comité de Regulación Ferroviaria y Aeroportuaria cuantas menciones se contengan en la normativa aplicable en relación con la Autoridad Estatal de Supervisión regulada en el Título VI, Capítulo IV, de la Ley 21/2003, de 7 de julio.

Asimismo, las menciones contenidas en la normativa vigente al Comité de Regulación Ferroviaria deberán entenderse realizadas al Comité de Regulación Ferroviaria y Aeroportuaria.

5. El ejercicio temporal de estas funciones, más allá de lo previsto en esta Disposición, no alterará lo previsto en los artículos 82 a 84 de la Ley 39/2003, de 17 de noviembre, del Sector Ferroviario.

6. La presente atribución temporal de funciones se prolongará asimismo una vez constituida la Comisión Nacional de los Mercados y la Competencia, y finalizará en el momento de la puesta en funcionamiento de dicha Comisión.

**Disposición adicional decimoséptima.** *Fomento de la corregulación publicitaria.*

La Comisión Nacional de los Mercados y la Competencia podrá firmar acuerdos de corregulación que coadyuven el cumplimiento de los objetivos establecidos en esta Ley, en particular, en relación con el control del cumplimiento de las obligaciones, las prohibiciones y los límites al ejercicio del derecho a realizar comunicaciones comerciales audiovisuales, con aquellos sistemas de autorregulación publicitaria que cumplan lo previsto en el artículo 37.4 de la Ley 3/1991, de 10 de enero, de competencia desleal. En el acuerdo se determinarán los efectos reconocidos a las actuaciones del sistema de autorregulación.

**Disposición adicional decimoctava.** *Otras sedes.*

La Comisión Nacional de los Mercados y la Competencia podrá tener otras sedes, de acuerdo con lo establecido en el apartado 3 del artículo 2 de esta Ley.

Su ubicación se realizará manteniendo la actualmente existente para las telecomunicaciones, donde se situará la Dirección de Telecomunicaciones del Sector Audiovisual (Instrucción de Telecomunicación y Servicios Audiovisuales), para el aprovechamiento de los recursos e infraestructuras actuales.

**Disposición adicional decimonovena.**

El Consejo de la Comisión Nacional de los Mercados y la Competencia, a propuesta de la persona titular de su Presidencia, aprobará un Código de Conducta del personal de la Comisión Nacional de los Mercados y la Competencia, que será publicado en el "Boletín Oficial del Estado" y que, sin perjuicio de la aplicación de las normas al respecto, podrá incluir disposiciones concretas en relación con los conflictos de intereses del personal del organismo.

**Disposición transitoria primera.** *Primer mandato de los miembros de la Comisión Nacional de Mercados y la Competencia.*

1. En la primera sesión del Consejo se determinarán, preferentemente de forma voluntaria y supletoriamente por sorteo, los tres consejeros que cesarán transcurrido el plazo de dos años desde su nombramiento y los tres que cesarán transcurrido el plazo de cuatro años.

2. No obstante lo dispuesto en el artículo 15 de esta Ley, los miembros del Consejo afectados por la primera renovación parcial podrán ser reelegidos por un nuevo mandato de seis años.

**Disposición transitoria segunda.** *Nombramiento del primer Presidente y Vicepresidente.*

Lo establecido en la Disposición transitoria primera de esta Ley no afectará al nombramiento del primer Presidente y Vicepresidente del organismo que, de acuerdo con el artículo 15.2 de la misma, tendrán un mandato de seis años no renovable.

**Disposición transitoria tercera.** *Continuación de funciones por los organismos que se extinguen.*

Desde la constitución de la Comisión Nacional de los Mercados y la Competencia hasta su puesta en funcionamiento, los organismos supervisores continuarán ejerciendo las funciones que desempeñan actualmente. Durante este periodo los miembros del Consejo permanecerán en su cargo en funciones y los organismos tendrán plena capacidad para desempeñar su actividad.

**Disposición transitoria cuarta.** *Desempeño transitorio de funciones por la Comisión Nacional de los Mercados y la Competencia.*

En relación con las funciones que, conforme a lo establecido en esta Ley, deban traspasarse a los ministerios, la Comisión Nacional de los Mercados y la Competencia, una vez haya entrado en funcionamiento, las desempeñará hasta el momento en el que los departamentos ministeriales dispongan de los medios necesarios para ejercerlas de forma efectiva.

**Disposición transitoria quinta.** *Procedimientos iniciados con anterioridad a la entrada en vigor de esta Ley.*

1. Los procedimientos iniciados con anterioridad a la entrada en vigor de esta Ley continuarán tramitándose por los órganos de la autoridad a los que esta Ley atribuye las funciones anteriormente desempeñadas por los organismos extinguidos.

2. La constitución y puesta en funcionamiento de la Comisión Nacional de los Mercados y la Competencia se podrá considerar una circunstancia extraordinaria que, conforme a la legislación específica aplicable, permitirá la ampliación del plazo máximo para resolver los procedimientos sometidos a caducidad o afectados por el silencio administrativo.

**Disposición transitoria sexta.** *Puestos de trabajo de personal funcionario que venían siendo desempeñados por personal laboral.*

Con carácter excepcional, el personal laboral fijo de los organismos públicos extintos que viniese ocupando puestos con funciones que, de acuerdo con lo establecido en esta Ley, deban ser desempeñadas por personal funcionario, podrá seguir ocupando dichos puestos.

Asimismo, los puestos que se puedan crear, así como los que queden vacantes, deberán ajustar su naturaleza a las previsiones del régimen jurídico de personal del artículo 31 de esta Ley.

**Disposición transitoria séptima.** *Presupuestos aplicables hasta la aprobación de los presupuestos de la Comisión Nacional de los Mercados y la Competencia.*

Una vez constituida la Comisión Nacional de los Mercados y la Competencia, en tanto en cuanto no disponga de un presupuesto propio, se mantendrán los presupuestos de los organismos que, de conformidad con la Disposición adicional segunda, queden extinguidos.

**Disposición transitoria octava.** *Régimen transitorio contable y de rendición de cuentas anuales.*

1. Las operaciones ejecutadas durante el ejercicio 2013 por la Comisión Nacional de los Mercados y la Competencia se registrarán en la contabilidad y el presupuesto de cada uno de los organismos extinguidos, según el ámbito al que correspondan dichas operaciones.

2. El Presidente de la Comisión Nacional de los Mercados y la Competencia formulará y aprobará por cada uno de los organismos extinguidos una cuenta del ejercicio 2013 que incluirá las operaciones realizadas por cada organismo y las indicadas en el apartado 1 anterior, procediendo también a su rendición al Tribunal de Cuentas en los términos que se establecen en la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

3. La formulación y aprobación de las cuentas anuales del ejercicio 2012 de los organismos extinguidos y su rendición al Tribunal de Cuentas en los términos que se establecen en la Ley 47/2003, de 26 de noviembre, General Presupuestaria, corresponderá a los cuentadantes de dichos organismos o al Presidente de la Comisión Nacional de los Mercados y la Competencia, si ésta ya se hubiera constituido.

**Disposición transitoria novena.** *Gestión y liquidación de las tasas previstas en el Anexo.*

1. La gestión y liquidación de las tasas a que se refiere el apartado I.1, en sus epígrafes A) y B), del Anexo de esta Ley se ajustarán, en tanto no se proceda a su nueva regulación, a lo establecido en la Orden FOM/3447/2010, de 29 de diciembre, por la que se aprueban los modelos de impresos para el pago de las tasas establecidas y reguladas en la Ley 23/2007, de 8 de octubre, de creación de la Comisión Nacional del Sector Postal.

2. La gestión y liquidación de las tasas a que se refiere el apartado I.4 del Anexo de esta Ley se ajustará, en tanto el Ministerio de Industria, Energía y Turismo no disponga de los medios necesarios para ejercer sus funciones de forma efectiva, a lo establecido en la Disposición adicional duodécima de la Ley 34/1998, de 7 de octubre.

**Disposición transitoria décima.** *Órganos de asesoramiento de la Comisión Nacional de Energía.*

Los órganos de asesoramiento de la Comisión Nacional de Energía previstos en la Disposición adicional undécima de la Ley 34/1998, de 7 de octubre, seguirán ejerciendo sus funciones hasta que se constituya el Consejo Consultivo de Energía previsto en la Disposición adicional decimoquinta de esta Ley.

**Disposición derogatoria.**

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en esta Ley y de manera específica:

a) El apartado 7 de la Disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.

b) La Disposición adicional undécima, excepto el apartado sexto, que permanece vigente, y la Disposición adicional duodécima de la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos.

c) El artículo 48 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, a excepción de su apartado 4.

d) Los artículos 82, 83 y 84 de la Ley 39/2003, de 17 de noviembre, del Sector Ferroviario.

e) Los artículos 12, 17 y 40 y el Título III de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

f) La Ley 23/2007, de 8 de octubre, de creación de la Comisión Nacional del Sector Postal.

g) El Título V de la Ley 7/2010, de 31 de marzo, General de Comunicación Audiovisual.

h) El Capítulo II del Título I y la Disposición final cuarta de la Ley 2/2011, de 4 de marzo, de Economía Sostenible.

i) El artículo 20, los apartados 15 y 16 del artículo 21, los artículos 25, 26, 27, 28, 29, 30, 31, 32 y 33, el apartado 2 del artículo 34, la Disposición transitoria quinta y el párrafo primero de la Disposición final segunda de la Ley 13/2011, de 27 de mayo, de Regulación del Juego.

j) El Real Decreto-Ley 11/2011, de 26 de agosto, por el que se crea la Comisión de Regulación Económica Aeroportuaria, se regula su composición y se modifica el régimen jurídico del personal laboral de AENA.

**Disposición final primera.** *Modificación de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.*

El apartado 1 de la Disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, se modifica en los siguientes términos:

> «1. La Comisión Nacional del Mercado de Valores, el Consejo de Seguridad Nuclear, las Universidades no transferidas, la Agencia Española de Protección de Datos, el Consorcio de la Zona Especial Canaria, la Comisión Nacional de los Mercados y la Competencia, el Museo Nacional del Prado y el Museo Nacional Centro de Arte Reina Sofía se regirán por su legislación específica y supletoriamente por esta Ley.»

**Disposición final segunda.** *Modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.*

El apartado 5 de la Disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, se modifica en los siguientes términos:

> «5. Los actos y disposiciones dictados por la Agencia Española de Protección de Datos, Comisión Nacional de los Mercados y la Competencia, Consejo Económico y Social, Instituto Cervantes, Consejo de Seguridad Nuclear, Consejo de Universidades y Sección Segunda de la Comisión de Propiedad Intelectual, directamente, ante la Sala de lo Contencioso-Administrativo de la Audiencia Nacional.»

**Disposición final tercera.** *Modificación de la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos.*

El apartado 4 del artículo 116 queda modificado como sigue:

> «4. La Comisión Nacional de Energía será competente para imponer sanciones en los siguientes casos:
>
> a) Infracciones muy graves previstas en el artículo 109.1.h), i), q), r) y ac).
>
> Asimismo, podrá imponer sanciones en el caso de las infracciones tipificadas en los párrafos d), g) y j) del artículo 109.1 siempre y cuando la infracción se produzca por la negativa al cumplimiento de decisiones jurídicamente vinculantes, remisión de información o realización de inspecciones y otros requerimientos de la Comisión Nacional de Energía en el ámbito de sus competencias y en el caso de infracciones tipificadas en el párrafo ab) cuando afecte a materias de su competencia.
>
> b) Infracciones graves prevista en el artículo 110.l, t), u) y w).
>
> Asimismo, podrá imponer sanciones en el caso de las infracciones tipificadas en los párrafos d) y f) del artículo 110, siempre y cuando la infracción se produzca por la

negativa al cumplimiento de decisiones jurídicamente vinculantes, remisión de información o realización de inspecciones y otros requerimientos de la Comisión Nacional de Energía en el ámbito de sus competencias y en el caso de infracciones tipificadas en el párrafo v) cuando afecte a materias de su competencia.

c) Infracciones leves en relación con incumplimientos de decisiones jurídicamente vinculantes y requerimientos de la Comisión Nacional de Energía en el ámbito de sus competencias.»

**Disposición final cuarta.** *Modificación de la Ley 21/2003, de 7 de julio, de Seguridad Aérea.*

La Ley 21/2003, de 7 de julio, de Seguridad Aérea, queda modificada como sigue:

Uno. Se añade una nueva Disposición adicional decimotercera, con la siguiente redacción:

**«Disposición adicional decimotercera.** *Régimen jurídico del personal laboral de Aena.*

La negociación colectiva, la contratación y el régimen jurídico del personal laboral de la Entidad Pública Empresarial Aena que no tenga la condición de controlador de tránsito aéreo será el legalmente establecido para el personal de Aena Aeropuertos, S.A.»

Dos. Se añade una nueva Disposición adicional decimocuarta, con la siguiente redacción:

**«Disposición adicional decimocuarta.** *Procedimientos en materia de tarifas aeroportuarias.*

1. En el caso de inadmisión de la propuesta cuando ésta se haya efectuado prescindiendo del procedimiento contemplado en el artículo 98 de esta Ley, se concederá al gestor aeroportuario un plazo para subsanar las deficiencias detectadas, transcurrido el cual sin que se hayan subsanado o manteniéndose las condiciones de inadmisión de la propuesta, la Comisión Nacional de los Mercados y la Competencia remitirá la propuesta de modificación tarifaria que considere razonable, debidamente justificada y en la que consten las irregularidades identificadas, al órgano competente para su incorporación al anteproyecto de ley que corresponda.

En otro caso, la constatación de irregularidades en el procedimiento de consulta y transparencia previsto en el artículo 98 de esta Ley dará lugar a la emisión de recomendaciones de la Comisión Nacional de los Mercados y la Competencia sobre las medidas a adoptar en futuras consultas, incluida la necesidad de ampliarlas a las compañías usuarias del aeropuerto no asociadas a las asociaciones u organizaciones representativas de usuarios.

2. En el ejercicio de la función de supervisión de que las propuestas de modificación o actualización de las tarifas aeroportuarias presentadas por el gestor aeroportuario se ajustan a lo previsto en los artículos 91 y 101.1 de esta Ley, la Comisión Nacional de los Mercados y la Competencia remitirá al órgano competente para su inclusión en el anteproyecto de Ley que corresponda, las propuestas del gestor aeroportuario que cumplan con dichos criterios.

En otro caso, la Comisión comunicará al gestor aeroportuario la modificación tarifaria revisada o, en su caso, los criterios que habría de seguir para que la propuesta garantice el cumplimiento de lo dispuesto en el párrafo anterior y el plazo para presentar la nueva propuesta ajustada a dichos criterios. Recibida la comunicación del gestor aeroportuario o transcurrido el plazo concedido al efecto sin haberla obtenido, la Comisión remitirá la modificación tarifaria revisada que proceda al órgano competente para su inclusión en el anteproyecto de ley que corresponda. En la propuesta de la Comisión se hará constar de forma clara y precisa la

modificación tarifaria propuesta por dicha Comisión así como el punto de vista del gestor aeroportuario.

En el establecimiento de la modificación tarifaria revisada, la Comisión procurará evitar fluctuaciones excesivas de las tarifas aeroportuarias, siempre y cuando sea compatible con los principios establecidos en el artículo 91 y 101.1 de esta Ley.»

Tres. Se añade una nueva Disposición adicional decimoquinta con la siguiente redacción:

**«Disposición adicional decimoquinta.** *Consulta sobre tarifas aeroportuarias.*

En aquéllos aeropuertos en los que los usuarios de aeronaves de aviación general o deportiva, trabajos aéreos y de aeronaves históricas tengan una presencia significativa se dará participación en el procedimiento de consulta a que se refieren los artículos 98 y 102 a las asociaciones u organizaciones representativas de dichos operadores.»

**Disposición final quinta.** *Modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, queda modificada como sigue:

Uno. El artículo 13 bis queda redactado en los siguientes términos:

**«Artículo 13 bis.** *Separación funcional.*

1. Cuando la Comisión Nacional de los Mercados y la Competencia llegue a la conclusión de que las obligaciones impuestas, en virtud de lo dispuesto en el artículo anterior, no han bastado para conseguir una competencia efectiva y que sigue habiendo problemas de competencia o fallos del mercado importantes y persistentes en relación con mercados al por mayor de productos de acceso, podrá decidir la imposición, como medida excepcional, a los operadores con poder significativo en el mercado integrados verticalmente, de la obligación de traspasar las actividades relacionadas con el suministro al por mayor de productos de acceso a una unidad empresarial que actúe independientemente.

Esa unidad empresarial suministrará productos y servicios de acceso a todas las empresas, incluidas otras unidades empresariales de la sociedad matriz, en los mismos plazos, términos y condiciones, en particular en lo que se refiere a niveles de precios y de servicio, y mediante los mismos sistemas y procesos.

2. Cuando la Comisión Nacional de los Mercados y la Competencia se proponga imponer una obligación de separación funcional, elaborará una propuesta que incluya:

a) pruebas que justifiquen las conclusiones a las que ha llegado,

b) pruebas de que hay pocas posibilidades, o ninguna, de competencia basada en la infraestructura en un plazo razonable,

c) un análisis del impacto previsto sobre la autoridad reguladora, sobre la empresa, particularmente en lo que se refiere a los trabajadores de la empresa separada y al sector de las comunicaciones electrónicas en su conjunto, sobre los incentivos para invertir en el sector en su conjunto, en especial por lo que respecta a la necesidad de garantizar la cohesión social y territorial, así como sobre otras partes interesadas, incluido en particular el impacto previsto sobre la competencia en infraestructuras y cualquier efecto negativo potencial sobre los consumidores, y

d) un análisis de las razones que justifiquen que esta obligación es el medio más adecuado para aplicar soluciones a los problemas de competencia o fallos del mercado que se hayan identificado.

3. El proyecto de medida incluirá los elementos siguientes:

a) la naturaleza y el grado precisos de la separación, especificando en particular el estatuto jurídico de la entidad empresarial separada,

b) una indicación de los activos de la entidad empresarial separada y de los productos o servicios que debe suministrar esta entidad,

c) los mecanismos de gobernanza para garantizar la independencia del personal empleado por la entidad empresarial separada y la estructura de incentivos correspondiente,

d) las normas para garantizar el cumplimiento de las obligaciones,

e) las normas para garantizar la transparencia de los procedimientos operativos, en particular de cara a otras partes interesadas, y

f) un programa de seguimiento para garantizar el cumplimiento, incluida la publicación de un informe anual.

4. La propuesta de imposición de la obligación de separación funcional, una vez que el Ministerio de Industria, Energía y Turismo y el Ministerio de Economía y Competitividad, como Autoridades Nacionales de Reglamentación identificadas en el apartado 1 del artículo 46, hayan emitido informe sobre la misma, se presentará a la Comisión Europea.

5. Tras la decisión de la Comisión Europea, la Comisión Nacional de los Mercados y la Competencia llevará a cabo, de conformidad con el procedimiento previsto en el artículo 10, un análisis coordinado de los distintos mercados relacionados con la red de acceso. Sobre la base de su evaluación, previo informe del Ministerio de Industria, Energía y Turismo, la Comisión Nacional de los Mercados y la Competencia impondrá, mantendrá, modificará o suprimirá las obligaciones correspondientes.

6. En el supuesto de que una empresa designada como poseedora de poder significativo en uno o varios mercados pertinentes, se proponga transferir sus activos de red de acceso local, o una parte sustancial de los mismos, a una persona jurídica separada de distinta propiedad, o establecer una entidad empresarial separada para suministrar a todos los proveedores minoristas, incluidas sus propias divisiones minoristas, productos de acceso completamente equivalentes, deberá informar con anterioridad al Ministerio de Industria, Energía y Turismo, al Ministerio de Economía y Competitividad y a la Comisión Nacional de los Mercados y la Competencia. Las empresas informarán también al Ministerio de Industria, Energía y Turismo, al Ministerio de Economía y Competitividad y a la Comisión Nacional de los Mercados y la Competencia de cualquier cambio de dicho propósito, así como del resultado final del proceso de separación.

En este caso, la Comisión Nacional de los Mercados y la Competencia evaluará el efecto de la transacción prevista sobre las obligaciones reglamentarias impuestas a esa entidad, llevando a cabo, de conformidad con el procedimiento previsto en el artículo 10, un análisis coordinado de los distintos mercados relacionados con la red de acceso. Sobre la base de su evaluación, previo informe del Ministerio de Industria, Energía y Turismo, la Comisión Nacional de los Mercados y la Competencia impondrá, mantendrá, modificará o suprimirá las obligaciones correspondientes.

7. Las empresas a las que se haya impuesto o que hayan decidido, la separación funcional podrán estar sujetas a cualquiera de las obligaciones enumeradas en el artículo 13 en cualquier mercado de referencia en que hayan sido designadas como poseedoras de poder significativo en el mercado.»

Dos. El apartado 1 del Anexo 1 queda redactado en los siguientes términos:

«1. Tasa general de operadores.

1. Sin perjuicio de la contribución económica que pueda imponerse a los operadores para la financiación del servicio universal, de acuerdo con lo establecido en el artículo 25 y en el Título III, todo operador estará obligado a satisfacer una tasa anual que no podrá exceder el 1,5 por mil de sus ingresos brutos de explotación y que estará destinada a sufragar los gastos que se generen, incluidos los de gestión, control y ejecución, por la aplicación del régimen jurídico establecido en esta Ley, por las autoridades nacionales de reglamentación a que se refiere el artículo 68.

A efectos de lo señalado en el párrafo anterior, se entiende por ingresos brutos el conjunto de ingresos que obtenga el operador derivados de la explotación de las redes y la prestación de los servicios de comunicaciones electrónicas incluidos en el ámbito de aplicación de esta Ley. A tales efectos, no se considerarán como ingresos brutos los correspondientes a servicios prestados por un operador cuyo importe recaude de los usuarios con el fin de remunerar los servicios de operadores que exploten redes o presten servicios de comunicaciones electrónicas.

2. La tasa se devengará el 31 de diciembre de cada año. No obstante, si por causa imputable al operador, éste perdiera la habilitación para actuar como tal en fecha anterior al 31 de diciembre, la tasa se devengará en la fecha en que esta circunstancia se produzca.

3. El importe de esta tasa anual no podrá exceder de los gastos que se generen, incluidos los de gestión, control y ejecución, por la aplicación del régimen jurídico establecido en esta Ley, anteriormente referidos.

A tal efecto, el Ministerio de Industria, Energía y Turismo hará pública antes del 30 de abril de cada año una memoria que contenga los gastos en que han incurrido en el ejercicio anterior las autoridades nacionales de reglamentación a que se refiere el artículo 68 por la aplicación del régimen jurídico establecido en esta Ley.

La memoria contemplará, de forma separada, los gastos en los que haya incurrido la Comisión Nacional de los Mercados y la Competencia por la aplicación del régimen jurídico establecido en esta Ley, que servirán de base para fijar la asignación anual de la Comisión con cargo a los Presupuestos Generales del Estado y garantizar la suficiencia de recursos financieros de la Comisión para la aplicación de esta Ley.

El importe de la tasa resultará de aplicar al importe de los gastos en que han incurrido en el ejercicio anterior las autoridades nacionales de reglamentación a que se refiere el artículo 68 por la aplicación del régimen jurídico establecido en esta Ley y que figura en la citada memoria, el porcentaje que individualmente representan los ingresos brutos de explotación de cada uno de los operadores de telecomunicaciones en el ejercicio anterior sobre el total de los ingresos brutos de explotación obtenidos en ese mismo ejercicio por los operadores de telecomunicaciones.

Reglamentariamente se determinará el sistema de gestión para la liquidación de esta tasa y los plazos y requisitos que los operadores de telecomunicaciones deben cumplir para comunicar al Ministerio de Industria, Energía y Turismo el importe de sus ingresos brutos de explotación con el objeto de que éste calcule el importe de la tasa que corresponde satisfacer a cada uno de los operadores de telecomunicaciones.»

Tres. El apartado 5 del Anexo I queda redactado en los siguientes términos:

«5. Gestión y recaudación en período voluntario de las tasas.

El Ministerio de Industria, Energía y Turismo gestionará y recaudará en período voluntario las tasas de este Anexo.»

**Disposición final sexta.** *Modificación de la Ley 39/2003, de 17 de noviembre, del Sector Ferroviario.*

La Ley 39/2003, de 17 de noviembre, del Sector Ferroviario, queda modificada como sigue:

Uno. El artículo 95, queda redactado en los siguientes términos:

**«Artículo 95.** *Competencia para la imposición de sanciones.*

Corresponderá la imposición de las sanciones por infracciones leves a los Delegados del Gobierno en las Comunidades Autónomas y por infracciones graves al Secretario de Estado de Infraestructuras, Transporte y Vivienda del Ministerio de

Fomento. Las sanciones por infracciones muy graves serán impuestas por el Ministro de Fomento.

Corresponde a la Comisión Nacional de los Mercados y la Competencia la imposición de las sanciones por el incumplimiento de sus resoluciones tipificado como infracción en los artículos 88.b) y 89.a).»

Dos. Se añade un nuevo apartado 12 al artículo 96 con la siguiente redacción:

«12. Las actuaciones reguladas en este artículo serán realizadas por la Comisión Nacional de los Mercados y la Competencia cuando se trate de procedimientos incoados como consecuencia de las infracciones a las que se refiere el párrafo segundo del artículo 95.»

**Disposición final séptima.** *Modificación de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.*

Se añade un nuevo apartado 3 en el artículo 70 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia, con la siguiente redacción:

«3. La recaudación de las multas corresponderá a la Administración General del Estado en periodo voluntario y a la Agencia Estatal de Administración Tributaria en período ejecutivo, conforme a lo establecido en el Reglamento General de Recaudación aprobado por el Real Decreto 939/2005, de 29 de julio.»

**Disposición final octava.** *Modificación de la Ley 54/1997, de 27 de noviembre, del Sector Eléctrico.*

Uno. Se suprime el apartado 7 del artículo 13 de la Ley 54/1997, de 27 de noviembre, del Sector Eléctrico.

Dos. Se modifica el apartado 3 del artículo 66 de la Ley 54/1997, de 27 de noviembre, del Sector Eléctrico, que queda redactado como sigue:

«3. La Comisión Nacional de los Mercados y la Competencia, dentro de su ámbito de actuación y de las funciones que tiene encomendadas, podrá imponer sanciones efectivas, proporcionadas y disuasorias a las empresas eléctricas por las infracciones administrativas tipificadas como muy graves en los números 1, 2, 5, 6 y 7 del artículo 60.a) de la presente Ley, así como por aquellas tipificadas en los números 8, 9 y 10 del citado artículo 60.a), en relación con los incumplimientos de resoluciones jurídicamente vinculantes o requerimientos de la Comisión Nacional de los Mercados y la Competencia en el ámbito de sus competencias.

Asimismo, la Comisión Nacional de los Mercados y la Competencia tendrá competencia para sancionar la comisión de las infracciones graves a que se hace referencia en el párrafo anterior cuando, por las circunstancias concurrentes, no puedan calificarse de muy graves y, en particular, en el caso de las tipificadas en los números 4, 5 y 22 del artículo 61.a) de la presente Ley, en relación con los incumplimientos de resoluciones jurídicamente vinculantes o requerimientos de la citada Comisión en el ámbito de sus competencias.

La Comisión Nacional de los Mercados y la Competencia tendrá competencia para sancionar aquellas infracciones leves tipificadas en el artículo 62 de la presente Ley, en relación con los incumplimientos de resoluciones jurídicamente vinculantes o requerimientos de la Comisión Nacional de los Mercados y la Competencia en el ámbito de sus competencias.

En cualquier caso la cuantía de la sanción no podrá superar el 10% del importe neto anual de la cifra de negocios del gestor de la red de transporte a dicho gestor, o el 10% del importe neto anual de la cifra de negocios consolidada de la sociedad matriz del grupo verticalmente integrado a dicha empresa integrada verticalmente, según los casos.»

**Disposición final novena.** *Título competencial.*

Esta Ley se dicta al amparo de lo dispuesto en:

a) El artículo 149.1.13ª de la Constitución, que atribuye al Estado la competencia exclusiva para dictar las bases y coordinación de la planificación general de la actividad económica.

b) El artículo 149.1.20ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de aeropuertos de interés general.

c) El artículo 149.1.21ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de ferrocarriles que transcurran por el territorio de más de una Comunidad Autónoma; régimen general de comunicaciones; correos y telecomunicaciones.

d) El artículo 149.1.25ª de la Constitución, que atribuye al Estado la competencia exclusiva para dictar las bases del régimen minero y energético.

e) El artículo 149.1.27ª de la Constitución, que atribuye al Estado la competencia exclusiva para dictar legislación básica del régimen de prensa, radio y televisión.

**Disposición final décima.** *Habilitación normativa.*

1. El Gobierno podrá dictar las disposiciones reglamentarias necesarias para el desarrollo y aplicación de esta Ley.

2. En el plazo máximo de dos meses desde la entrada en vigor de esta Ley, el Consejo de Ministros aprobará mediante real decreto, el Estatuto Orgánico a que hace referencia el artículo 26 de esta Ley, en el que se establecerán cuantas cuestiones relativas al funcionamiento y régimen de actuación de la Comisión Nacional de los Mercados y la Competencia resulten necesarias conforme a las previsiones de esta Ley y, en particular, las siguientes:

a) La estructura orgánica de la Comisión Nacional de los Mercados y la Competencia.

b) La distribución de competencias entre los distintos órganos.

c) El régimen de su personal.

**Disposición final undécima.** *Entrada en vigor.*

Esta Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

## ANEXO

### Tasas y prestaciones patrimoniales de carácter público relacionadas con las actividades y servicios regulados en esta Ley

*I. Tasas por prestación de servicios y realización de actividades*

1. Tasas por prestación de servicios y realización de actividades en relación con el sector postal

A) Tasa por inscripción en el Registro General de empresas prestadoras de servicios postales.

1. Hecho imponible.

Constituye el hecho imponible de la tasa la inscripción y renovación de la inscripción en el Registro General de empresas prestadoras de servicios postales.

2. Devengo.

La tasa se devengará con la inscripción y renovación anual de la misma.

3. Sujetos pasivos.

Serán sujetos pasivos las personas físicas o jurídicas que presten servicios postales y figuren inscritas en el Registro General de empresas prestadoras de servicios postales.

Las empresas que presten simultáneamente servicios postales incluidos en el ámbito del servicio postal universal y servicios no incluidos en dicho ámbito, deberán estar inscritas en el Registro General de empresas prestadoras de servicios postales en las secciones

correspondientes a tales servicios. Cada acto de inscripción y de renovación dará lugar al abono de la tasa pertinente.

4. Cuantías.

La cuota a ingresar será de 275 euros, que deberá abonarse en el momento en que se realice la inscripción en el Registro o la renovación de la misma.

5. Gestión.

La liquidación de la tasa por el Ministerio de Fomento se ajustará a lo que se disponga en orden ministerial dictada al efecto.

B) Tasa por la expedición de certificaciones registrales.

1. Hecho imponible.

Constituye el hecho imponible de la tasa la expedición de certificaciones registrales emitidas por el Registro General de empresas prestadoras de servicios postales.

No será aplicable la tasa en el caso de certificaciones emitidas con ocasión de la inscripción inicial o renovación de la misma en dicho Registro.

2. Devengo.

La tasa se devengará con la solicitud de la certificación registral.

3. Sujetos pasivos.

Serán sujetos pasivos las personas que soliciten la certificación.

4. Cuantías.

La cuota a ingresar será de 100 euros, que deberá abonarse de forma simultánea a la presentación de la solicitud.

5. Gestión.

La liquidación de la tasa por el Ministerio de Fomento se ajustará a lo que se disponga en orden ministerial dictada al efecto.

C) Tasas por la concesión de autorizaciones administrativas singulares.

La liquidación de la tasa por el Ministerio de Fomento seguirá exigiéndose en los términos establecidos en el artículo 32 de la Ley 43/2010, de 30 de diciembre, del servicio postal universal, de los derechos de los usuarios y del mercado postal.

2. Tasas por prestación de servicios y realización de actividades en relación con las operaciones de concentración

Tasa por análisis y estudio de las operaciones de concentración.

1. Hecho imponible.

Constituye el hecho imponible de la tasa la realización, por la Comisión Nacional de los Mercados y de la Competencia, del análisis de las concentraciones sujetas a control de acuerdo con el artículo 8 de la Ley 15/2007, de 3 de julio, de Defensa la Competencia.

2. Devengo.

La tasa se devengará con la presentación de la notificación prevista en el artículo 9 de la Ley 15/2007, de 3 de julio.

Si se presentare la autoliquidación sin ingreso, se procederá a su exacción por la vía de apremio, sin perjuicio de que la Comisión Nacional de los Mercados y la Competencia instruya el correspondiente expediente.

3. Sujetos pasivos.

Serán sujetos pasivos las personas que resulten obligadas a notificar de acuerdo con el artículo 9 de la Ley 15/2007, de 3 de julio.

4. Cuantías.

1.º Una cuota fija de 1.500 euros para aquellas concentraciones que requieran su tramitación a través del formulario abreviado de notificación previsto en el artículo 56 de la Ley 15/2007, de 3 de julio. No obstante, si la Comisión Nacional de los Mercados y la Competencia decide, conforme a lo establecido en el artículo mencionado, que las partes deben presentar el formulario ordinario, éstas deberán realizar la liquidación complementaria correspondiente.

2.º En el supuesto de análisis de operaciones de concentración económicas sujetas a control de acuerdo con el artículo 8 de la Ley 15/2007, de 3 de julio, la cuota de la tasa será:

a) De 5.502,15 euros cuando el volumen de negocios global en España del conjunto de los partícipes en la operación de concentración sea igual o inferior a 240.000.000 de euros.

b) De 11.004,31 euros cuando el volumen de negocios global en España de las empresas partícipes sea superior a 240.000.000 de euros e igual o inferior a 480.000.000 de euros.

c) De 22.008,62 euros cuando el volumen de negocios global en España de las empresas partícipes sea superior a 480.000.000 de euros e igual o inferior a 3.000.000.000 de euros.

d) De una cantidad fija de 43.944 euros cuando el volumen de negocios en España del conjunto de los partícipes sea superior a 3.000.000.000 de euros, más 11.004,31 euros adicionales por cada 3.000.000.000 de euros en que el mencionado volumen de negocios supere la cantidad anterior, hasta un límite máximo de 109.806 euros.

5. Devolución.

De conformidad con lo previsto en el artículo 12 de la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, la devolución de tasas exigidas solo procederá cuando el hecho imponible no se hubiere realizado por causas no imputables al sujeto pasivo.

6. Gestión.

La liquidación de la tasa por la Comisión Nacional de los Mercados y la Competencia se ajustará a lo que se disponga en la orden ministerial dictada al efecto.

3. Tasas por prestación de servicios y realización de actividades en relación con el sector de las telecomunicaciones

Corresponderá al Ministerio de Industria, Energía y Turismo la liquidación de las siguientes tasas:

A) Tasa general de operadores, regulada en el apartado 1 del Anexo I de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

B) Tasas por numeración telefónica, reguladas en el apartado 2 del Anexo I de la Ley 32/2003, de 3 de noviembre.

C) Tasa por reserva del dominio público radioeléctrico, reguladas en el apartado 3 del Anexo I de la Ley 32/2003, de 3 de noviembre.

D) Tasas de telecomunicaciones, reguladas en el apartado 4 del Anexo I de la Ley 32/2003, de 3 de noviembre.

4. Tasas previstas para el ejercicio de las funciones del sector energético

1. A los efectos previstos en la presente Ley, se establecen las siguientes tasas:

Primero. Tasa aplicable a la prestación de servicios y realización de actividades en relación con el sector de hidrocarburos líquidos.

a) Hecho imponible. Constituye el hecho imponible de la tasa la prestación de servicios y realización de actividades por el Ministerio de Industria, Energía y Turismo en relación con el sector de los hidrocarburos líquidos, de conformidad con lo establecido en esta Ley y en la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos.

b) Base imponible. La base imponible de la tasa viene constituida por las ventas anuales de gasolinas, gasóleos, querosenos, fuelóleos y gases licuados del petróleo a granel y

envasado expresadas en toneladas métricas (Tm), cuya entrega se haya realizado en territorio nacional. A estos efectos, no tendrán la consideración de ventas las realizadas entre operadores, ni las ventas realizadas por los operadores a los que se refiere el artículo 45 de la Ley 34/1998, de 7 de octubre, a distribuidores de gases licuados del petróleo por canalización a consumidores finales.

Las ventas a que se refiere el párrafo anterior se calcularán anualmente, con base en las realizadas en el año natural anterior y se aplicarán a partir del 1 de enero. Mediante resolución de la Dirección General de Política Energética y Minas del Ministerio de Industria, Energía y Turismo se determinarán las ventas anuales que corresponden a cada operador y que servirán de base para el cálculo de la cuota tributaria a ingresar en el Tesoro Público. En tanto en cuanto no se dicte la resolución a que se refiere el párrafo anterior, el Ministerio de Industria, Energía y Turismo efectuará la liquidación prevista en la letra f) de este apartado conforme a las ventas anuales establecidas para el ejercicio inmediatamente anterior. Una vez dictada la resolución por la Dirección General de Política Energética y Minas del Ministerio de Industria, Energía y Turismo, éste efectuará las regularizaciones que, en su caso, procedan de acuerdo con la determinación de ventas que la misma hubiese establecido.

c) Devengo de la tasa. La tasa se devengará el día último de cada mes natural.

d) Sujetos pasivos. Los sujetos pasivos de la tasa son los operadores al por mayor a que se refieren los artículos 42 y 45 de la Ley 34/1998, de 7 de octubre.

e) Tipo de gravamen y cuota. El tipo por el que se multiplicará la base imponible para determinar la cuota tributaria a ingresar en el Tesoro Público será de 0,140817 euros/Tm.

f) Normas de gestión. La tasa será objeto de liquidación mensual por el Ministerio de Industria, Energía y Turismo, ascendiendo el importe de cada liquidación practicada a la doceava parte de la cuota tributaria definida en la letra e) anterior.

El ingreso de la tasa liquidada y notificada por el Ministerio de Industria, Energía y Turismo se realizará por los sujetos pasivos definidos en la letra d) anterior en los plazos fijados en el Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio.

Segundo. Tasa aplicable a la prestación de servicios y realización de actividades en relación con el sector de hidrocarburos gaseosos.

a) Hecho imponible. Constituye el hecho imponible de la tasa la prestación de servicios y realización de actividades por el Ministerio de Industria, Energía y Turismo y por la Comisión Nacional de los Mercados y la Competencia en el sector de los hidrocarburos gaseosos, de conformidad con lo establecido en esta Ley y en la Ley 34/1998, de 7 de octubre, del sector de hidrocarburos.

b) Base imponible. La base imponible de la tasa viene constituida por la facturación total derivada de la aplicación de peajes y cánones a que se refiere el artículo 92 de la Ley 34/1998, de 7 de octubre.

c) Devengo. La tasa se devengará el día último de cada mes natural.

d) Sujetos pasivos. Los sujetos pasivos de la tasa son las empresas que realicen las actividades de regasificación, almacenamiento en tanques de GNL, almacenamiento básico, transporte y distribución, en los términos previstos en la Ley 34/1998, de 7 de octubre.

e) Tipos de gravamen y cuota. El tipo por el que se multiplicará la base imponible para determinar la cuota tributaria a ingresar en el Tesoro Público será de 0,140 por ciento.

f) Normas de gestión. La tasa será objeto de autoliquidación mensual por los sujetos pasivos definidos en la letra d) anterior. El sujeto pasivo cumplimentará el correspondiente impreso de declaración-liquidación, según los modelos que apruebe mediante Resolución el Ministerio de Industria, Energía y Turismo.

A los efectos previstos en el párrafo anterior, antes del día 25 de cada mes, los sujetos pasivos deberán presentar al Ministerio de Industria, Energía y Turismo declaración-liquidación sobre la facturación total correspondiente al mes anterior, con desglose de períodos y facturas.

El plazo para el ingreso de las tasas correspondientes a la facturación de cada mes, será, como máximo, el día 10, o el siguiente día hábil, del mes siguiente al siguiente a aquel a que se refiera el período de facturación liquidado.

g) Integración de la tasa en la estructura de peajes y cánones prevista en la Ley 34/1998, de 7 de octubre. La tasa por prestación de servicios y realización de actividades en el sector de hidrocarburos gaseosos tiene la consideración de coste permanente del sistema gasista, integrándose a todos los efectos en la estructura, peajes y cánones establecida por la Ley 34/1998, de 7 de octubre, y disposiciones de desarrollo de la misma.

Tercero. Tasa aplicable a la prestación de servicios y realización de actividades en relación con el sector eléctrico.

a) Hecho imponible. Constituye el hecho imponible de la tasa la prestación de servicios y realización de actividades por el Ministerio de Industria, Energía y Turismo y por la Comisión Nacional de los Mercados y la Competencia en relación con el sector eléctrico, de conformidad con lo establecido en esta Ley y en la Ley 54/1997, de 27 de noviembre, del Sector Eléctrico.

b) Exenciones y bonificaciones. En materia de exenciones y bonificaciones se estará a lo establecido en la Disposición adicional única del Real Decreto 2017/1997, de 26 de diciembre, por el que se organiza y regula el procedimiento de liquidación de los costes de transporte, distribución y comercialización a tarifa, de los costes permanentes del sistema y de los costes de diversificación y seguridad de abastecimiento, por la que se determina el régimen de exenciones y coeficientes reductores aplicable a las cuotas a que se refiere el artículo 5 del citado Real Decreto.

Asimismo, resultará de aplicación lo dispuesto en la Disposición transitoria sexta del citado Real Decreto 2017/1997, de 26 de diciembre.

c) Base imponible. La base imponible de la tasa viene constituida por la facturación total derivada de la aplicación de los peajes de acceso a que se refiere el artículo 17 de la Ley 54/1997, de 27 de noviembre.

d) Devengo de la tasa. La tasa se devengará el día último de cada mes natural.

e) Sujetos pasivos. Los sujetos pasivos de la tasa son las empresas que desarrollan las actividades de transporte y distribución, en los términos previstos en la Ley 54/1997, de 27 de noviembre.

f) Tipos de gravamen y cuota. El tipo por el que se multiplicará la base imponible para determinar la cuota tributaria a ingresar en el Tesoro Público será de 0,150 por ciento, para los peajes a que se refiere el artículo 17 de la Ley 54/1997, de 27 de noviembre.

g) Normas de gestión. La tasa será objeto de autoliquidación mensual por los sujetos pasivos definidos en la letra e) anterior. El sujeto pasivo cumplimentará el correspondiente impreso de declaración-liquidación, según los modelos que apruebe mediante resolución el Ministerio de Industria, Energía y Turismo.

A los efectos previstos en el párrafo anterior, antes del día 25 de cada mes, los sujetos pasivos deberán presentar al Ministerio de Industria, Energía y Turismo declaración-liquidación sobre la facturación total correspondiente al mes anterior, con desglose de periodos y facturas.

El ingreso de las tasas correspondientes a la facturación del penúltimo mes anterior se realizará antes del día 10 de cada mes o, en su caso, del día hábil inmediatamente posterior.

h) Integración de la tasa en la estructura de peajes prevista en la Ley 54/1997, de 27 de noviembre. La tasa por prestación de servicios y realización de actividades en el sector eléctrico tiene la consideración de coste permanente del sistema, en los términos previstos en el artículo 16.5 de la Ley 54/1997, de 27 de noviembre, integrándose a todos los efectos en la estructura de peajes establecida por la citada Ley y disposiciones de desarrollo de la misma.

2. La gestión y recaudación en período voluntario de las tasas definidas en la presente Disposición corresponderá al Ministerio de Industria, Energía y Turismo, en los términos previstos en la Ley 58/2003, de 17 de diciembre, General Tributaria y demás normativa de aplicación.

La competencia para acordar el aplazamiento y fraccionamiento de pago en período voluntario de las tasas definidas en la presente Disposición, corresponderá, asimismo, al Ministerio de Industria, Energía y Turismo, según lo previsto en el Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio. La recaudación en vía

ejecutiva será competencia de los órganos de recaudación de la Hacienda Pública, de acuerdo con lo previsto en la normativa tributaria.

3. En lo no previsto en los apartados anteriores será de aplicación lo establecido en la Ley 58/2003, de 17 de diciembre, General Tributaria, en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos y normas de desarrollo de las mismas.

4. Los tipos de gravamen serán revisados por el Gobierno con carácter cuatrienal, adaptándolos a las necesidades de financiación que justifiquen la Comisión Nacional de los Mercados y la Competencia y el Ministerio de Industria, Energía y Turismo.

La primera revisión se realizará al año siguiente en que el Ministerio de Industria, Energía y Turismo ejerza de forma efectiva las funciones encomendadas en la Disposición adicional octava de esta Ley.

5. La prestación de servicios y realización de actividades por el Ministerio de Industria, Energía y Turismo a que se hace referencia en los apartados Primero a), Segundo a) y Tercero a) incluirá aquellos realizados por organismos adscritos al mismo a los que el citado Ministerio encomiende la prestación o realización de los servicios y actividades.

6. En las leyes de presupuestos generales del Estado de cada año se determinará qué porcentaje de lo recaudado por las tasas previstas en los apartados Segundo y Tercero se destinará a la Comisión Nacional de los Mercados y la Competencia para el ejercicio de sus funciones en el ámbito del sector energético.

5. Tasa por la gestión administrativa del juego

La gestión de esta tasa será realizada por el Ministerio de Hacienda y Administraciones Públicas.

*II. Prestaciones patrimoniales de carácter público*

1. Aportaciones a realizar por los operadores de telecomunicaciones y por los prestadores privados del servicio de comunicación audiovisual televisiva, de ámbito geográfico estatal o superior al de una Comunidad Autónoma, reguladas en los artículos 5 y 6 de la Ley 8/2009, de 28 de agosto, de financiación de la Corporación Radio y Televisión Española.

2. Contribución postal regulada en el artículo 31 de la Ley 43/2010, de 30 de diciembre.