Orden TES/369/2023, de 10 de abril, por la que se aprueba la Política de Seguridad de la Información y de los Servicios en el ámbito de la administración digital del Ministerio de Trabajo y Economía Social y se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Departamento.

Ministerio de Trabajo y Economía Social
«BOE» núm. 91, de 17 de abril de 2023
Referencia: BOE-A-2023-9290

TEXTO CONSOLIDADO
Última modificación: sin modificaciones

El marco de relación entre la Administración Pública y los ciudadanos a través de los medios electrónicos se encuentra establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Por su parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público define, en su artículo 156, el objeto del Esquema Nacional de Seguridad (ENS) y lo incorpora como parte esencial en la configuración del archivo electrónico de los documentos regulado en el artículo 46 y en el régimen de relaciones electrónicas y transferencias de tecnología entre las Administraciones Públicas, tal como establece su artículo 158.

Ambas normas han sido objeto de desarrollo mediante 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.

La administración digital debe ser confiable para que los ciudadanos realicen los trámites administrativos correspondientes con total seguridad y fiabilidad. Para ello, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, persigue alcanzar una protección adecuada de la información tratada y de 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.

En particular, el artículo 12.3 del citado Real Decreto 311/2022, de 3 de mayo, establece que, en la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento.

La política de seguridad de la información constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el ENS.

Además, la política de seguridad de la información debe ser coherente con lo establecido 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.

En el ámbito del Ministerio de Trabajo y Economía Social se debe garantizar la seguridad como un proceso integral de cada etapa del ciclo de vida de cada sistema de información, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Además, el sistema de información debe estar preparado para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con lo que prevé el Esquema Nacional de Seguridad.

Mediante el Real Decreto 2/2020, de 12 de enero, por el que se reestructuran los departamentos ministeriales, fue creado el Ministerio de Trabajo y Economía Social. Posteriormente, se aprobaron el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales, y el Real Decreto 499/2020, de 28 de abril, por el que se desarrolla la estructura orgánica básica del Ministerio de Trabajo y Economía Social, y se modifica el Real Decreto 1052/2015, de 20 de noviembre, por el que se establece la estructura de las Consejerías de Empleo y Seguridad Social en el exterior y se regula su organización, funciones y provisión de puestos de trabajo.

El marco normativo vigente en el ámbito de la prestación de servicios electrónicos a los ciudadanos, en materia de política de seguridad de la información y de protección de datos personales, así como la actual organización administrativa determinan la necesidad de dictar esta orden por la que se aprueba la política de seguridad de la información y de los servicios en el ámbito de la administración digital del Ministerio de Trabajo y Economía Social y se crea, en este Departamento, el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones.

Esta orden cumple con los principios de buena regulación, de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia recogidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

En primer lugar, en virtud de los principios de necesidad y eficacia, esta iniciativa normativa está justificada por las razones expuestas y es el instrumento más adecuado para dar cumplimiento al mandato contenido en el artículo 12.3 del citado Real Decreto 311/2022, de 3 de mayo. Además, se ajusta al principio de proporcionalidad, en tanto que la norma contiene la regulación imprescindible para atender sus objetivos. Se garantiza el principio de seguridad jurídica, en tanto que la norma es coherente con el resto del ordenamiento jurídico y, en particular, con el marco regulatorio en el ámbito de la política de seguridad de la información. Cumple con el principio de transparencia, ya que identifica claramente su propósito y, al tratarse de una norma organizativa su tramitación no ha requerido de la consulta pública previa ni de los trámites de audiencia e información pública. Finalmente, es también adecuada al principio de eficiencia, ya que no impone cargas administrativas.

La orden se ha desarrollado también en el marco de lo dispuesto en la disposición adicional primera de la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales (LOPD) y del artículo 32 del Reglamento UE 2016/679, del Parlamento Europeo y del Consejo (RGPD) en orden a aplicar las medidas de seguridad al tratamiento de datos personales.

En el proceso de su tramitación, ha sido informada por la Agencia Española de Protección de Datos y por la Comisión Ministerial de Administración Digital del Ministerio de Trabajo y Economía Social.

En su virtud, con la aprobación previa de la Ministra de Hacienda y Función Pública, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. El objeto de esta orden ministerial es la aprobación de la Política de Seguridad de la Información y de los Servicios (en adelante Política de Seguridad o PSI), en el ámbito de la Administración Digital del Ministerio de Trabajo y Economía Social, así como la creación del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social y la regulación de su composición, funcionamiento y funciones.

2. La Política de Seguridad establece las orientaciones o directrices que rigen la actuación en el Ministerio de Trabajo y Economía Social, de las personas y entidades, en relación con la seguridad de los sistemas de información; entendiendo que un Sistema de Información es un conjunto organizado de recursos (físicos, lógicos, de comunicación, de datos, procedimientos y personas) que permite conseguir las especificaciones funcionales establecidas para el Departamento. La Política de Seguridad aprobada en esta orden ministerial se aplicará a todos los sistemas de información del Ministerio de Trabajo y Economía Social.

La PSI es de obligado cumplimiento para todo el personal que acceda a los sistemas de información y a la información del Departamento y para los órganos superiores y directivos del Ministerio de Trabajo y Economía Social y de sus organismos públicos adscritos, que no tengan establecida su propia política de seguridad.

En caso de discrepancia con las políticas de seguridad que pudieran estar definidas de manera específica para tales órganos y organismos públicos, prevalecerá la definida en esta orden ministerial.

Artículo 2. *Misión del Departamento.*

Corresponde al Ministerio de Trabajo y Economía Social la propuesta y ejecución de la política del Gobierno en materia de empleo, de relaciones laborales, de economía social y de responsabilidad social de las empresas, de acuerdo con lo establecido en el Real Decreto 499/2020, de 28 de abril, por el que se desarrolla la estructura orgánica básica del Ministerio de Trabajo y Economía Social, y se modifica el Real Decreto 1052/2015, de 20 de noviembre, por el que se establece la estructura de las Consejerías de Empleo y Seguridad Social en el exterior y se regula su organización, funciones y provisión de puestos de trabajo.

Artículo 3. *Marco normativo.*

1. El marco normativo en que se desarrollan las actividades del Ministerio de Trabajo y Economía Social en el ámbito de la prestación de los servicios electrónicos a la ciudadanía, sin perjuicio de la legislación específica, está integrado fundamentalmente por las siguientes disposiciones:

a) 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).

b) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

c) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

d) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

e) Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

f) 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.

g) 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.

h) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

i) Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

j) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en al ámbito de la Administración Electrónica.

k) 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.

l) 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.

2. También forman parte del marco normativo las restantes normas aplicables a la administración electrónica del Departamento derivadas de las anteriores y publicadas en las sedes electrónicas dentro del ámbito de aplicación de la PSI.

3. El Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social mantendrá actualizado dicho marco normativo, especialmente las instrucciones técnicas de seguridad, de obligado cumplimiento, esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el Esquema Nacional de Seguridad.

Artículo 4. *Principios de la Política de Seguridad.*

1. La política de seguridad aplicará los principios básicos que se establecen en el ENS en el ámbito de la Administración electrónica, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permitiendo una protección adecuada de la información y de los servicios.

2. Atendiendo al ENS, el Ministerio de Trabajo y Economía Social implementará diversas medidas de seguridad proporcionales a la naturaleza de la información y de los servicios a proteger, teniendo en cuenta la categoría de los sistemas afectados bajo los siguientes principios:

a) Protección de datos personales. Se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de datos de carácter personal.

b) Alcance estratégico. La seguridad de la información en el que deberá contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas del Departamento para conformar un todo coherente y eficaz.

c) Seguridad Integral. La seguridad constituirá un proceso integral compuesto por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema basado en la mejora continua de todos ellos y del proceso en sí mismo.

d) Análisis y gestión de riesgos: Todos los sistemas afectados por la PSI, así como todos los tratamientos de datos personales, serán objeto de un análisis de riesgos que evalúe las amenazas y los riesgos a los que están expuestos. Este análisis, que deberá ajustarse, en todo caso, a un criterio de proporcionalidad a los riesgos potenciales y la criticidad y valor de la información y de los servicios afectados, y de acuerdo con los artículos 24, 25 y 32 del RGPD, el artículo 28 de la LOPD y 3 del RD 311/2022, cuando el sistema de información trate datos personales, se realizará:

1.º Regularmente, al menos una vez al año, revisando la situación del Sistema de Información para determinar si se han producido cambios que requieran una actualización en materia de seguridad.

2.º Cuando cambie la información manejada o los servicios prestados de manera significativa.

3.º Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

e) Prevención, reacción, recuperación y mejora continua. Se implementará un proceso integral de prevención, reacción y recuperación frente a incidentes de seguridad con procedimientos de detección, análisis, comunicación, resolución y registro de las actuaciones para la mejora continua de la seguridad de los sistemas, designando un punto de contacto para las comunicaciones con respecto a incidentes detectados y estableciendo protocolos para el intercambio de información relacionada con el incidente, incluyendo las comunicaciones con los Equipos de Respuesta a Emergencias (CERT).

f) Líneas de defensa. Se implementará una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falla, el sistema implementado permitirá ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse; reducir la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

g) Reevaluación periódica e integridad y actualización del sistema. Se implementarán controles y evaluaciones regulares y periódicas de la seguridad (de forma interna o con la ayuda de terceros) para conocer en todo momento el estado de la seguridad de los sistemas con el objeto de adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

h) Función diferenciada: El Ministerio de Trabajo y Economía Social organizará su seguridad comprometiendo a todos los miembros del Departamento mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el artículo 6. Estos controles, así como los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

En los supuestos de tratamientos de datos personales se identificará además a la persona, organismo o unidad responsable del tratamiento y, en su caso, al encargado de tratamiento, de acuerdo con los dispuesto en el artículo 4, apartados 7 y 8 del RGPD.

Artículo 5. *Requisitos de la seguridad de la información.*

Tal y como establece el ENS, la política de seguridad debe desarrollarse aplicando una serie de requisitos mínimos:

a) Organización e implantación del proceso de seguridad. La seguridad deberá comprometer a todo el personal del Ministerio de Trabajo y Economía Social.

b) Análisis y gestión de los riesgos. Se realizará una gestión de los riesgos consistente en un proceso de identificación, análisis, evaluación y tratamiento a los que el sistema esté expuesto. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Cuando un sistema de información trate datos personales, la persona responsable o encargada del tratamiento, asesorada por la persona delegada de protección de datos, realizará 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.

El análisis y la gestión deberá realizarse de acuerdo con las previsiones del artículo 15 de la presente orden ministerial, adaptando los criterios de determinación del riesgo en el tratamiento de los datos conforme a lo establecido en el artículo 32 del RGPD y, en caso necesario, estableciendo niveles de seguridad más altos.

c) Gestión de personal y profesionalidad. Se establecerá un programa de concienciación continua anual para formar a todos los empleados públicos que prestan servicio en su ámbito, en particular, a los de nueva incorporación. Del mismo modo, las personas con responsabilidad concreta en el uso, operación o administración de sistemas TIC recibirán formación específica para el manejo seguro de los sistemas en la medida en que la necesitan para realizar su trabajo. La formación será obligatoria antes de asumir una nueva responsabilidad, tanto si es la primera asignación como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

d) Autorización y control de los accesos. Se implementarán mecanismos de control de acceso al sistema general de información, limitándolos a los estrictamente necesarios y debidamente autorizados. Los sistemas de información individuales se diseñarán de forma que garanticen la seguridad por defecto, proporcionando la mínima funcionalidad requerida para alcanzar los objetivos y priorizando el uso sencillo, de tal forma que una utilización insegura requiera, en todo caso, de un acto consciente por parte del usuario. Tales sistemas de información individuales serán solo accesibles por las personas o desde emplazamientos o equipos autorizados, pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.

e) Protección de las instalaciones. Se implementarán mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

f) Adquisición de productos. Ante cualquier adquisición, el Ministerio de Trabajo y Economía Social tendrá en cuenta que dichos productos tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen.

g) Seguridad por defecto. Los sistemas deberán diseñarse y configurarse de forma que garanticen la seguridad por defecto. El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos. Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que solo son accesibles por las personas, o desde emplazamientos o equipos, autorizados.

Cuando el sistema afecte a datos personales, la adopción de medidas de seguridad por defecto y desde el diseño deberá realizarse de acuerdo con los artículos 24 y 25 del RGPD.

h) Integridad y actualización del sistema. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

i) Protección de la información almacenada y en tránsito. Se implementarán mecanismos para proteger la información almacenada o en tránsito, especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.). Los sistemas dispondrán de los medios de protección de la información almacenada y en tránsito (copias de seguridad y otros mecanismos necesarios), que garanticen la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

j) Prevención ante otros sistemas de información interconectados. La estrategia de protección protegerá el perímetro, en particular, si se conecta a redes públicas. En todo caso, analizará los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas y se controlará su punto de unión.

k) Registro de actividad. Se habilitarán registros de la actividad de las personas usuarias reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de las personas afectadas, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral y demás disposiciones que resulten de aplicación.

l) Incidentes de seguridad. Se establecerá un sistema de detección y reacción frente a código dañino.

m) La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el RGPD, la LOPD, en especial su disposición adicional primera, así como el resto de la normativa de aplicación.

Se deberán implementar medios organizativos y materiales que, en los supuestos de violación de la seguridad de los datos personales, garanticen la notificación a la autoridad de control, la documentación del incidente y la comunicación a los interesados, en su caso, requiriendo para ello la implicación del delegado de protección de datos.

n) Continuidad de la actividad. Los sistemas de información del Ministerio de Trabajo y Economía Social dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

o) Mejora continua del proceso de seguridad. El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua.

p) Auditoría de la seguridad. Se promoverá las auditorías de los sistemas de información de manera regular, al menos cada dos años, para que se verifique el cumplimiento de los requerimientos del Esquema Nacional de Seguridad, siguiendo la normativa vigente en función de la categoría de cada sistema de información.

Artículo 6. *Estructura organizativa para la gestión de la seguridad.*

La estructura organizativa para la gestión de la seguridad de los sistemas de información del Ministerio de Trabajo y Economía Social está compuesta por:

a) El Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones (COSTIC).

b) Las personas responsables de los sistemas de información.

c) Las personas responsables de la información y de los servicios.

d) Las personas responsables de la seguridad.

e) La persona designada como delegada de protección de datos.
f) Las personas responsables del tratamiento de datos personales.
g) Las personas encargadas del tratamiento de datos personales.
h) Las personas responsables de la prestación de los servicios TIC.

Artículo 7. *El Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social.*

1. Se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social, en adelante COSTIC, como órgano colegiado de carácter transversal, adscrito a la Subsecretaría de Trabajo y Economía Social con la siguiente composición:

a) Presidencia: La persona titular de la Subsecretaría de Trabajo y Economía Social.
b) Vicepresidencia: La persona titular de la Dirección del Gabinete Técnico de la Subsecretaría.
c) Vocalías:

1.º Un representante designado por la persona titular de la Secretaría de Estado de Empleo y Economía Social, con rango mínimo de subdirector general o asimilado.
2.º Un representante designado por la persona titular de la Subsecretaría de Trabajo y Economía Social, con rango mínimo de subdirector general o asimilado.
3.º La persona titular de la Subdirección General de Tecnologías de la Información y Comunicaciones, que, además, actuará como secretaria del COSTIC.
4.º La persona responsable de la seguridad del Ministerio.
5.º La persona responsable de la seguridad del Servicio Público de Empleo Estatal (SEPE).
6.º La persona responsable de la seguridad del Fondo de Garantía Salarial (FOGASA).
7.º La persona responsable de la seguridad del Instituto Nacional de Seguridad y Salud en el Trabajo (INSST).
8.º La persona responsable de la seguridad del Organismo Estatal de la Inspección de Trabajo y Seguridad Social (OEITSS).

2. La persona designada como delegada de protección de datos participará con voz, pero sin voto, en las reuniones del COSTIC, cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación.
3. En casos de vacante, ausencia, enfermedad, abstención, recusación u otra causa legal, la persona a la que corresponda la Presidencia será sustituida por la persona titular de la Vicepresidencia. La persona que ostente la Secretaría del órgano será sustituida, en su caso, por el vocal designado por la persona titular de la Subsecretaría. En el caso de las vocalías, las personas que las desempeñen serán sustituidas por quienes designe el órgano que ha designado a las titulares.
4. Con carácter opcional, en función de los asuntos a tratar, otros miembros del Ministerio de Trabajo y Economía Social podrán incorporarse a las labores del Comité, incluyendo las personas responsables de la información, de los servicios, de los sistemas de información y grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

Artículo 8. *Funciones del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social.*

Al COSTIC le corresponden las siguientes funciones:

a) Proponer revisiones y actualizaciones de la Política de Seguridad y de las normas de seguridad.
b) Mantener actualizado el marco normativo aplicable a la seguridad de los sistemas de información.
c) Proponer planes de mejora de la seguridad de los sistemas de información, que podrán contemplar la aprobación, revisión y mejora de los planes estratégicos, los planes directores, los procedimientos, las normas y las líneas de actuación del Departamento en materia de seguridad de los sistemas de información, con su dotación presupuestaria

correspondiente, priorizando las actuaciones en materia de seguridad, cuando los recursos sean limitados.

d) Promover, aprobar, revisar y mejorar las políticas de auditoría, en especial del ENS y de la protección de datos personales, de las unidades del Departamento.

e) Aprobar las declaraciones de aplicabilidad y conformidad con el ENS.

f) Realizar un seguimiento de los principales riesgos residuales e incidentes de seguridad y recomendar posibles actuaciones respecto a ellos.

g) Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y, en particular, en materia de protección de datos de carácter personal.

h) Definir los mecanismos y resolver los conflictos entre las personas con roles de seguridad asignados.

Artículo 9. *Organización y funcionamiento del Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo y Economía Social.*

1. El COSTIC se reunirá con carácter ordinario una vez al año y con carácter extraordinario cuando su presidente así lo convoque.

2. El COSTIC se podrá constituir, convocar, celebrar sus reuniones, adoptar acuerdos y remitir actas, tanto de forma presencial como a distancia, de conformidad con los artículos 17 y 18 de la Ley 40/2015, de 1 de octubre.

3. La Secretaría del COSTIC levantará acta de las reuniones, siendo enviadas a la Presidencia de dicho comité para su aprobación, en su caso, en el pleno siguiente. Esta Secretaría realizará, junto con la persona responsable de la seguridad del Departamento, todos los trabajos previos necesarios para las reuniones del COSTIC, apoyándose cuando lo requiera en las unidades y organismos del Departamento.

Corresponde a la Secretaría del COSTIC la revisión de la Política de Seguridad, al menos anualmente, proponiendo mejoras de esta y presentándola para su toma en consideración por parte del COSTIC, así como la actualización del marco normativo aplicable y la revisión de las normas de seguridad con la ayuda de las personas responsables de seguridad.

4. El COSTIC se regirá por esta orden y por las normas previstas para los órganos colegiados en la sección 3.ª del capítulo II del título preliminar de la Ley 40/2015, de 1 de octubre.

Artículo 10. *La persona responsable del sistema.*

1. La persona responsable del sistema es quien tiene la responsabilidad de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

2. Son funciones de la persona responsable del sistema:

a) Definir la tipología y sistema de gestión del sistema de información estableciendo los criterios de uso y los servicios disponibles en el mismo.

b) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

c) Proponer la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser adoptada por las personas responsables de la información afectada o del servicio afectado y la persona responsable de la seguridad.

d) Para las demás funciones que por su naturaleza así lo requieran, se coordinará con la Secretaría General Técnica; en particular, en lo relativo a las actuaciones de implementación, desarrollo y administración del Archivo Electrónico Único del Departamento.

3. La persona titular de la Subdirección General de Tecnologías de la Información y Comunicaciones actuará como responsable del sistema en el ámbito del Departamento. Cada uno de los organismos públicos adscritos al Ministerio, a los que sea de aplicación esta política de seguridad, designarán una persona o unidad responsable del sistema.

Artículo 11. *Las personas o unidades administrativas responsables de la información.*

1. Conforme a los artículos 13 y 41 del Real Decreto 311/2022, de 3 de mayo, es responsable de la información la persona o unidad administrativa que tiene la potestad de establecer los requisitos de la información tratada y su implicación en la valoración del sistema de información del que forme parte.

2. Serán funciones de la persona responsable de la información, dentro de su ámbito de actuación, las siguientes:

a) Establecer los requisitos de la información tratada.

b) Valorar el impacto que tendría un incidente que afectase a la seguridad de la información con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.

La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio y el respeto de la legalidad y de los derechos de los ciudadanos.

c) Aceptar los riesgos residuales respecto de la información, calculados en el análisis de riesgos.

d) Adoptar, de acuerdo con las personas responsables del servicio afectado y de seguridad, la decisión de la suspensión del manejo de una cierta información a propuesta de la persona responsable del sistema cuando haya sigo informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

3. La designación de la persona responsable de la información corresponderá a la persona titular de cada órgano superior o directivo dependiente del Ministerio y de cada uno de sus organismos públicos adscritos, a los que sea de aplicación esta política de seguridad, de acuerdo con su propia organización interna.

Artículo 12. *Las personas o unidades administrativas responsables de los servicios.*

1. Conforme a los artículos 13 y 41 Real Decreto 311/2022, de 3 de mayo, es responsable del servicio la persona o unidad administrativa, que tiene la potestad de establecer los requisitos del servicio prestado y su implicación en la valoración del nivel de seguridad de dicho servicio.

2. Serán funciones de la persona responsable del servicio, dentro de su ámbito de actuación las siguientes:

a) Determinar los requisitos de los servicios prestados.

b) Valorar el impacto que tendría un incidente que afectase a la seguridad de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad.

La valoración de las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

c) Aceptar los riesgos residuales respecto de los servicios, calculados en el análisis de riesgos.

d) Adoptar, de acuerdo con las personas responsables de la información y de seguridad, la decisión de la suspensión de la prestación de un cierto servicio a propuesta de la persona responsable del sistema cuando haya sigo informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

3. La designación de la persona responsable del servicio corresponderá a la persona titular de cada órgano superior o directivo dependiente del Ministerio y de cada uno de sus organismos públicos adscritos, a los que sea de aplicación esta política de seguridad, de acuerdo con su propia organización interna.

4. La persona responsable de la información y la responsable del servicio podrán coincidir en una misma persona o unidad administrativa.

Artículo 13. *La persona responsable de la seguridad.*

1. Conforme al artículo 13 del Real Decreto 311/2022, de 3 de mayo, la persona responsable de seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, y supervisa la implantación de las medidas necesarias para garantizar que se satisfacen dichos requisitos y reportar sobre estas cuestiones.

2. Serán funciones de la persona responsable de seguridad, dentro de su ámbito de actuación, las siguientes:

a) Mantener y verificar el nivel adecuado de seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Promover la formación y concienciación en materia de seguridad de la información.

c) Designar responsables de la ejecución del análisis de riesgos y de la declaración de aplicabilidad, identificar medidas de seguridad, determinar las configuraciones necesarias y elaborar la documentación del sistema.

d) Determinar la categoría de seguridad del sistema en colaboración con la persona responsable del sistema y con las responsables de la información y del servicio.

e) Participar en la elaboración e implantación de los planes de mejora de la seguridad y, en su caso, en la de los planes de continuidad, procediendo a su validación.

f) Gestionar y asegurar las revisiones externas o internas del sistema, incluyendo auditorías que serán transmitidas a las personas responsables de los sistemas de información para el seguimiento y resolución de las deficiencias encontradas.

g) Gestionar los procesos de certificación y las declaraciones de aplicabilidad pertinentes de los sistemas de información.

h) Generar y mantener actualizada la documentación relativa a su ámbito de responsabilidad.

i) Adoptar, de acuerdo con las personas responsables de la información y del servicio afectado, la decisión de la suspensión del manejo de una cierta información o la prestación de un cierto servicio a propuesta de la persona responsable del sistema cuando haya sido informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

3. La persona titular de la Subsecretaría designará a la persona responsable de seguridad del Ministerio. Asimismo, designará al responsable de seguridad de cada organismo público adscrito al Departamento, a propuesta del organismo correspondiente.

De acuerdo con lo previsto en el artículo 13.3 del Real Decreto 311/2022, de 3 de mayo, la persona responsable de la seguridad será distinta de la responsable del sistema, no debiendo existir dependencia jerárquica entre ambas. 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 del citado real decreto.

Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, la persona titular de la Subsecretaría podrá designar a las personas responsables de seguridad delegadas que considere necesarias, que tendrán dependencia funcional directa de la persona responsable de seguridad del Ministerio y que serán responsables, en su ámbito, de todas aquellas acciones que aquella les delegue.

Para garantizar que la persona responsable de seguridad no reciba instrucciones que limiten el desempeño de sus funciones, las desempeñará con independencia de las unidades que gestionen las tecnologías de la información y comunicaciones, y en estas funciones dependerá de la Presidencia del COSTIC.

Artículo 14. *Delegado de protección de datos.*

El delegado de protección de datos tiene carácter asesor y supervisor para el cumplimiento de lo dispuesto en el RGPD y demás normativa aplicable sobre protección de datos personales, debiéndose garantizar su independencia dentro de la organización y evitar

cualquier conflicto de intereses, así como proveer de los medios necesarios para el desarrollo de sus funciones conforme al artículo 39 del RGPD.

El asesoramiento y supervisión del delegado de protección de datos se extiende a aquellas medidas de seguridad que se quieran implementar con finalidades distintas a garantizar la protección de datos, en la medida que impliquen un tratamiento adicional de datos personales.

Dentro de la gestión general de incidentes, el delegado de protección de datos intervendrá en la gestión de las brechas de datos personales, principalmente en su posición de interlocutor de la persona responsable o encargada del tratamiento ante la Agencia Española de Protección de Datos.

Artículo 15. *Tratamiento de datos personales.*

1. Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Trabajo y Economía Social las medidas de seguridad apropiadas derivadas del análisis de riesgos de privacidad, así como de la evaluación de impacto relativa a la protección de datos, tal y como se detalla en el artículo 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

Cuando un sistema de información trate datos personales, la persona responsable o la encargada del tratamiento, asesoradas por la persona designada como delegada de protección de datos, realizarán un análisis de riesgos, conforme al artículo 24 del Reglamento General de Protección de Datos.

La identificación de los riesgos específicos para los derechos y libertades de las personas físicas en relación con los tratamientos efectuados por la entidad debe ser previo al análisis de riesgos de sistemas donde se implementen los tratamientos, con el fin de permitir que el sistema de seguridad sea adecuado al riesgo que los tratamientos suponen para los derechos y libertades de las personas.

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, la persona responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, de conformidad con lo establecido en el artículo 35 del RGPD.

Además, en cumplimiento de la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, se aplicarán las medidas de seguridad que correspondan de las previstas en el ENS, 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 RGPD.

En el caso de que el análisis de riesgos y la evaluación de impacto en su caso, determine medidas agravadas respecto a la normativa recogida en el anexo II del Real Decreto 311/2022, de 3 de mayo, dichas medidas serán las que se implementarán en la protección de datos personales.

2. En función de las diversas situaciones que puedan producirse en materia de protección de datos personales, se establecerá la oportuna coordinación con la persona designada como delegada de protección de datos, de conformidad con el artículo 37 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y el artículo 34 de la Ley Orgánica 3/2018 de 5 de diciembre, y, en la medida en que sea preciso, con las personas responsables y con las personas encargadas del tratamiento de datos personales.

Especialmente, se prestará apoyo a la persona designada como delegada de protección de datos, para la elaboración de propuestas o informes relativos a las reclamaciones de los interesados, comunicación de brechas de datos personales y respuestas a los requerimientos de la Agencia Española de Protección de Datos.

Artículo 16. *Normativa de seguridad.*

1. La normativa de seguridad del Ministerio de Trabajo y Economía Social se estructura en cuatro niveles siendo de obligada aplicación los tres primeros de la siguiente manera:

a) Primer nivel: La Política de Seguridad que queda regulada en esta orden ministerial.

b) Segundo nivel: Las normas de seguridad, instrucciones, protocolos, entre otros instrumentos, que concretan la Política de Seguridad y que deben especificar de forma concisa, transparente, inteligible y accesible, con un lenguaje claro y sencillo los objetivos de seguridad que se desean alcanzar.

c) Tercer nivel: Los procedimientos de seguridad, que se describen en los instrumentos referidos en el punto anterior, indican explícitamente y paso a paso cómo realizar una cierta actividad. Cada procedimiento debe detallar:

1.º En qué condiciones debe aplicarse.
2.º Quiénes son los que deben llevarlo a cabo.
3.º Qué es lo que hay que hacer en cada momento, incluyendo, en su caso, el registro de la actividad realizada.
4.º Cómo se miden sus resultados.
5.º Cómo se reportan posibles mejoras y deficiencias en los procedimientos.

d) Cuarto nivel: abarca la documentación de buenas prácticas, las recomendaciones formuladas y cualesquiera otros contenidos que afecten de manera no esencial a los conceptos constitutivos de los niveles anteriores.

Artículo 17. *Actuación y efectos respecto a la información correspondiente a otros entes o servicios de competencia ajena al Departamento.*

1. Cuando el Ministerio de Trabajo y Economía Social preste servicios a otros organismos o maneje información de otros organismos, se hará partícipes a los mismos de la política de seguridad. El Ministerio de Trabajo y Economía Social definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que el Departamento lleve a cabo en materia de seguridad en relación con otros organismos.

2. Cuando el Ministerio de Trabajo y Economía Social utilice servicios proporcionados por terceros o ceda información a terceros, se les hará partícipe de la política de seguridad y de la normativa de seguridad existente que atañe a dichos servicios o información. Estos sujetos que se relacionen con el Ministerio quedarán vinculados por las obligaciones establecidas en la mencionada normativa y podrán desarrollar sus propios procedimientos operativos para ejecutarlas. Se establecerán procedimientos específicos de comunicación y resolución de incidencias y se garantizará que su personal esté adecuadamente concienciado y formado en materia de seguridad.

3. Cuando algún aspecto de la política de seguridad no pueda ser satisfecho por una tercera parte según lo dispuesto en los párrafos anteriores, se requerirá un informe de la persona responsable de seguridad del Departamento u organismo adscrito al mismo, que precise los riesgos en los que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por las personas responsables de la información y de los servicios afectados antes de que la prestación de servicios o la cesión de la información continúen su ejecución.

4. Cuando la información contenga datos de carácter personal quedará sujeta a la normativa sobre protección de datos personales por la que están obligados a velar tanto las personas responsables como las encargadas del tratamiento.

Artículo 18. *Formación y concienciación.*

1. Todo el personal del Ministerio de Trabajo y Economía Social relacionado con la información, los servicios y los sistemas de información deberá conocer sus deberes y obligaciones en esta materia de seguridad de la información e identificar de forma inequívoca a las personas responsables de velar por su cumplimiento.

2. Para garantizar la seguridad de las tecnologías de la información aplicable a los sistemas y servicios del Ministerio de Trabajo y Economía Social, el COSTIC propondrá los mecanismos necesarios para desarrollar las actividades para la concienciación y la formación específica necesaria e imprescindible, en materia de política de seguridad de la información, en todos los niveles de la organización.

Disposición adicional única. *No incremento del gasto público.*

Las medidas incluidas en esta orden no supondrán incremento del gasto, y serán atendidas con los medios personales, técnicos y presupuestarios asignados al Ministerio de Trabajo y Economía Social.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas, en lo que afecta a las competencias del Ministerio de Trabajo y Economía Social, la Orden TIN/3016/2011, de 28 de octubre, por la que se crea el Comité de Seguridad de las Tecnologías de la Información y las Comunicaciones del Ministerio de Trabajo e Inmigración, y la Orden del Ministerio de Empleo y Seguridad Social, de 30 de julio de 2012, por la que se aprueba la Política de Seguridad de los Sistemas de Información del Ministerio de Empleo y Seguridad Social.

Disposición final primera. *Instrucciones de aplicación.*

La persona titular de la Subsecretaría de Trabajo y Economía Social podrá dictar las instrucciones necesarias para el adecuado cumplimiento de esta orden.

Disposición final segunda. *Publicidad de la Política de Seguridad.*

Esta orden se publicará en el «Boletín Oficial del Estado» y en la sede electrónica del Ministerio de Trabajo y Economía Social.

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».

Madrid, 10 de abril de 2023.–La Vicepresidenta Segunda del Gobierno y Ministra de Trabajo y Economía Social, Yolanda Díaz Pérez.