III. OTRAS DISPOSICIONES

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

12148 *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.*

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

cve: BOE-A-2021-12148
Verificable en https://www.boe.es

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».

Madrid, 7 de julio de 2021.–El Secretario General de Administración Digital, Juan Jesús Torres Carbonell.

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

cve: BOE-A-2021-12148
Verificable en https://www.boe.es

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.

cve: BOE-A-2021-12148
Verificable en https://www.boe.es

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.

cve: BOE-A-2021-12148
Verificable en https://www.boe.es

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.

cve: BOE-A-2021-12148
Verificable en https://www.boe.es

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.

cve: BOE-A-2021-12148
Verificable en https://www.boe.es

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.

cve: BOE-A-2021-12148
Verificable en https://www.boe.es