I. DISPOSICIONES GENERALES

MINISTERIO DE ASUNTOS EXTERIORES, UNIÓN EUROPEA Y COOPERACIÓN

17277 *Orden AUC/1147/2021, de 15 de octubre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración digital del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, y se modifica la Orden AEC/1372/2016, de 19 de julio, por la que se crea y regula la Comisión Ministerial para la Administración Digital del Ministerio de Asuntos Exteriores y de Cooperación.*

La Orden AEC/1647/2013, de 5 de septiembre, por la que se aprobó la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Asuntos Exteriores y de Cooperación (en adelante, PSI), identifica responsabilidades y establece el conjunto de principios y directrices básicos para una protección apropiada y consistente de los servicios y activos de información gestionados en el marco de competencias del Ministerio, generando así, de acuerdo con lo establecido en 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 adelante, ENS) en el ámbito de la Administración Electrónica, las condiciones necesarias de confianza en el uso de medios electrónicos.

Desde la aprobación de la citada PSI, se ha asistido a la modificación del marco normativo básico de aplicación en el ámbito de la administración electrónica. Se ha aprobado 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.

De igual forma, el 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, incorpora medidas para la seguridad pública, asegurando aspectos relacionados con la mayor exposición a ciberamenazas que exigen una mejor protección de redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano.

Asimismo, han entrado en vigor 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 la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Más recientemente, la transposición 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 (Directiva NIS) al ordenamiento jurídico español, se llevó a cabo mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y desarrollado a su vez por el 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. Esta norma legal regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales, estableciendo mecanismos que, con una perspectiva integral, permiten mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, y fijando un marco institucional de cooperación que facilita la coordinación de las

cve: BOE-A-2021-17277
Verificable en https://www.boe.es

actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea.

Por último, la reciente entrada en vigor del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por 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, que entre otros, persigue 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.

Además, este Ministerio ha elaborado el Plan de Acción Departamental para la Transformación Digital del Ministerio de Asuntos Exteriores y Cooperación, en cumplimiento de lo previsto en el Capítulo IV del 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. Adicionalmente, se han establecido nuevos procedimientos para reforzar la ciberseguridad en todo el Departamento.

Con el fin de adoptar la regulación existente a los cambios anteriormente descritos, se motiva la necesidad de establecer una PSI acorde a la situación actual.

En la elaboración de la orden se han cumplido los principios de buena regulación recogidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, y, en particular, los principios de necesidad y eficacia, pues se trata del instrumento óptimo para garantizar una política de seguridad en la utilización de medios electrónicos que permita una adecuada protección de la información dentro del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. También se adecúa al principio de proporcionalidad, pues no existe otra alternativa menos restrictiva de derechos o de obligaciones y, en cuanto a los principios de seguridad jurídica, transparencia y eficiencia, la norma es coherente con el resto del ordenamiento jurídico, y se ha debatido en el seno de la Comisión Permanente de la Comisión Ministerial para la Administración Digital, permitiendo una gestión más eficiente de los recursos públicos y no contempla cargas.

Esta orden ha sido informada por la Agencia Española de Protección de Datos, y por la Comisión Ministerial de Administración Digital del Departamento.

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

Artículo 1. *Objeto y ámbito de aplicación.*

1. Constituye el objeto de esta orden el establecer la Política de Seguridad de la Información (en lo sucesivo, PSI) en el ámbito de la administración digital del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, así como del marco normativo y organizativo de la misma.

2. La PSI será de obligado cumplimiento para todos los órganos superiores y directivos del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, incluidos los organismos adscritos al mismo que no tengan establecida su propia política de seguridad.

3. La PSI será aplicable a todos los activos empleados por el Departamento.

4. Se excluye del ámbito de esta orden las materias clasificadas, que se regirán por su propia política del manejo de la Información Clasificada.

Artículo 2. *Misión del departamento.*

Corresponde al Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, de conformidad con las directrices del Gobierno y en aplicación del principio de unidad de acción en el exterior, planificar, dirigir, ejecutar y evaluar la política exterior del Estado y la política de cooperación internacional para el desarrollo sostenible, con singular atención a las relacionadas con la Unión Europea y con Iberoamérica, y coordinar y

cve: BOE-A-2021-17277
Verificable en https://www.boe.es

supervisar todas las actuaciones que en dichos ámbitos realicen, en ejecución de sus respectivas competencias, los restantes Departamentos y Administraciones Públicas.

Asimismo, le corresponde fomentar las relaciones económicas, culturales y científicas internacionales; participar, en la esfera de actuación que le es propia, en la propuesta y aplicación de las políticas migratorias y de extranjería; fomentar la cooperación transfronteriza e interterritorial; proteger a los españoles en el exterior; y preparar, negociar y tramitar los Tratados Internacionales de los que España sea parte.

Artículo 3. *Marco legal y regulatorio de la seguridad de la información. .*

El marco normativo en que se desarrollan las actividades del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación en el ámbito de la prestación de los servicios electrónicos a los ciudadanos, sin perjuicio de la legislación específica, se compone de los siguientes textos normativos:

1. 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.
2. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
3. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
4. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
5. Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
6. 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.
7. 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.
8. 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.
9. 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.
10. Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021 de 30 de marzo.
11. 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.

Del mismo modo, forman parte del marco regulatorio la norma por la que se desarrolle la estructura orgánica básica del Departamento, las normas aplicables a la Administración Digital del Departamento, las normas aplicables en materia de protección de datos y cualquier norma de ciberseguridad que resulte de aplicación.

Artículo 4. *Principios de la seguridad de la información.*

1. Principios básicos.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

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

cve: BOE-A-2021-17277
Verificable en https://www.boe.es

b) Responsabilidad diferenciada: En los sistemas de información se diferenciará persona o unidad ministerial responsable de la información, que determina los requisitos de seguridad de la información tratada; responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; responsable del sistema, que tiene la responsabilidad técnica sobre la prestación de los servicios; y responsable de seguridad, que propone a la persona o unidad responsable de la información las decisiones para satisfacer los requisitos de seguridad. Las figuras de responsable de la información y responsable de servicio pueden recaer en la misma persona o unidad, en función de la estructura organizativa del servicio que se preste. En los supuestos de tratamientos de datos personales se identificará además a la persona o unidad responsable de tratamiento y, en su caso, al encargado de tratamiento, de acuerdo con el artículo 12 de esta orden.

c) Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.

d) Gestión de riesgos: de acuerdo con lo establecido en los artículos 24, 25 y 32 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, así como en el artículo 6 del Real Decreto 3/2010, de 8 de enero, el análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerán un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.

e) Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

f) Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido, dedicado y diferenciado.

g) Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto. En el ámbito del tratamiento de datos personales, deben cumplir con los principios de privacidad por defecto y desde el diseño.

2. Principios particulares y responsabilidades específicas.

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la PSI y que inspiran las actuaciones del Departamento en dicha materia. Se establecen los siguientes objetivos instrumentales:

a) Protección de datos de carácter personal: se adoptarán las medidas técnicas y organizativas necesarias para garantizar una adecuada protección de los datos. Tal y como establece en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, dichas medidas deberán ser apropiadas en función del análisis de riesgos mencionado en el artículo 4.1.d), así como de una evaluación de impacto en la protección de datos cuando sea probable que un tratamiento, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

cve: BOE-A-2021-17277
Verificable en https://www.boe.es

b) Gestión de activos de información: Los activos de información del Departamento se encontrarán inventariados y categorizados y estarán asociados a un responsable.

c) Seguridad ligada a las personas: se implantarán los mecanismos necesarios para que cualquier persona que acceda o pueda acceder a los activos de información conozca sus responsabilidades y, de este modo, se reduzca el riesgo derivado de un uso indebido de aquellos.

d) Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

k) Derechos y deberes de los empleados públicos: el personal empleado público que presta servicio al Departamento tiene el derecho y el deber de conocer y aplicar esta PSI y todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones, así como de participar en acciones de difusión y formación orientadas a mejorar el estado de la seguridad de la información y las medidas de seguridad para la protección de datos de carácter personal.

3. Aplicabilidad de los principios y requisitos mínimos marcados en el Esquema Nacional de Seguridad.

Sin perjuicio de lo establecido en los apartados 1 y 2 de este artículo, esta PSI se establecerá asimismo sobre la base de los principios básicos y se desarrollará aplicando los requisitos mínimos contemplados en los artículos 4 y 11 del Real Decreto 3/2010, de 8 de enero.

cve: BOE-A-2021-17277
Verificable en https://www.boe.es

Artículo 5. *Estructura organizativa de la Seguridad de la Información.*

La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación está compuesta por los siguientes agentes:

1. La Comisión Permanente de la Comisión Ministerial de Administración Digital (en adelante, CP-CMAD).
2. Responsables de la Información.
3. Responsables del Servicio.
4. Responsable de Seguridad.
5. Responsable del Sistema.
6. La persona delegada de Protección de Datos del Departamento y las personas delegadas de Protección de Datos de los Organismos adscritos.

Artículo 6. *La Comisión Permanente de la Comisión Ministerial de Administración Digital.*

1. La CP-CMAD es el órgano colegiado de ámbito departamental responsable del impulso y coordinación interna en materia de Administración Digital.
2. La CP-CMAD ejercerá las siguientes funciones en el gobierno de la Seguridad de la Información, aparte de las que le son conferidas en su orden ministerial de creación:

a) Elaborar las propuestas de modificación y actualización permanente de la PSI.
b) Velar e impulsar el cumplimiento de la PSI y de su desarrollo normativo.
c) Promover la mejora continua en la gestión de la seguridad de la información.
d) Nombrar formalmente a los distintos responsables mencionados en la estructura organizativa de esta PSI.
e) Resolver los posibles conflictos que puedan derivarse del establecimiento de la citada estructura organizativa.
f) Ordenar la realización de las auditorías o autoevaluaciones de seguridad y recibir información de los resultados de las mismas.
g) Proveer los recursos y medios necesarios para asegurar la concienciación y formación en materia de seguridad de la información de todo el personal afectado por esta orden.
h) Evaluación y seguimiento las decisiones tomadas para satisfacer los requisitos de seguridad de la información y de los servicios.
i) Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.
j) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la PSI y su normativa de desarrollo.

3. La Comisión Permanente de la CMAD podrá crear un Grupo de Trabajo para la elaboración de la documentación y recabar la información pertinente para la toma de sus decisiones en materia de la Seguridad de la Información.

Artículo 7. *Responsables de la Información y Responsables del Servicio.*

1. Las personas o unidades responsables de la información y aquellas responsables del servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos, en materia de seguridad, de los servicios y de la información que manejan.
2. Los órganos superiores o directivos del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, así como los organismos públicos adscritos al Departamento a los que, conforme al artículo 1, les sea de aplicación esta PSI, designarán estos perfiles de acuerdo con su propia organización interna. Se comunicarán los nombramientos al

cve: BOE-A-2021-17277
Verificable en https://www.boe.es

responsable de seguridad, para que pueda mantener el inventario mencionado en el artículo 8.3 d).

3. Las figuras de responsable de información y responsable de servicio pueden recaer en la misma persona o unidad en función de la estructura organizativa del servicio que se preste.

Artículo 8. *Responsable de Seguridad de la información.*

1. Conforme al artículo 10 del Real Decreto 3/2010 de 8 de enero, la persona o unidad responsable de seguridad es quien determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

2. Tanto el Departamento, como los organismos públicos adscritos al mismo a los que sea de aplicación esta PSI designarán una persona o unidad responsable de seguridad. El ámbito de actuación de cada responsable de seguridad se limitará única y exclusivamente a los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean competencia y responsabilidad directa del organismo al que pertenezca dicho responsable de seguridad.

3. Serán funciones del responsable de seguridad, las siguientes:

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

b) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

c) Impulsar el cumplimiento del cuerpo normativo definido en el artículo 11, así como velar por el mantenimiento de la documentación de seguridad y la gestión de mecanismos de acceso a la misma.

d) Mantener un inventario actualizado de las normas de primer y segundo nivel detalladas en el artículo 11, de los nombramientos derivados de esta orden, así como de los informes de auditorías, autoevaluaciones y análisis de riesgos realizados y de las declaraciones y certificaciones de seguridad.

e) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

f) Elaborar informes periódicos de seguridad que incluyan los incidentes más relevantes de cada período.

g) Promover la mejora continua en la gestión de la seguridad de la información.

h) Impulsar la formación y concienciación en materia de seguridad de la información.

i) Firmar la declaración de aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

j) Realizar los preceptivos análisis de riesgos, especialmente en el tratamiento de los datos de carácter personal, y mantenerlos actualizados según la legislación vigente.

k) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes de auditoría, elaborando las conclusiones a presentar a los responsables del servicio y los responsables de la Información para que adopten las medidas correctoras adecuadas bajo su responsabilidad.

l) Cualesquiera otras funciones que el Real Decreto 3/2010, de 8 de enero, asigne a las personas o unidades responsables de seguridad, así como las que viene a reforzar el Real Decreto 43/2021 de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre.

Artículo 9. *Responsable del Sistema.*

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

cve: BOE-A-2021-17277
Verificable en https://www.boe.es

2. En el ejercicio de las funciones de implementación y desarrollo de la política en materia de tecnologías de la información y comunicaciones en el ámbito del Ministerio, la persona titular de la Subdirección General Informática, Comunicaciones y Redes, actuará como responsable del sistema para todos aquellos activos de información que hayan sido sometidos a un proceso de consolidación de recursos TIC. En el resto de casos, cada unidad u organismo público adscrito al Departamento a los que, conforme al artículo 1, les sea de aplicación esta PSI, designará este perfil de acuerdo con su propia organización interna. Se comunicarán los nombramientos al responsable de seguridad, para que pueda mantener el inventario mencionado en el artículo 8.3.d).

Artículo 10. *La persona delegada de Protección de Datos.*

1. La persona delegada de Protección de Datos ejerce las funciones detalladas en la Sección 4 del Capítulo IV 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 en el Título V del Capítulo III de la Ley Orgánica 3/2018, de 5 de diciembre. Tendrá en todo caso acceso al registro de las actividades de tratamientos de datos de carácter personal al que se refiere el artículo 30 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

2. La designación de la persona delegada de Protección de Datos del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, y de los organismos adheridos a esta PSI se efectuará conforme con el artículo 37 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y del artículo 34 de la Ley Orgánica 3/2018 de 5 de diciembre. En consecuencia, será designada una persona atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones que tiene encomendadas. Se comunicarán los nombramientos a la persona o unidad responsable de seguridad, para que pueda mantener el inventario mencionado en el artículo 7.3.d).

3. La persona delegada de Protección de Datos estará adscrita a la Subsecretaría del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, correspondiendo sus funciones a la Inspección General de Servicios, y será única para todo el Departamento, sin perjuicio de la existencia de personas delegadas de Protección de Datos en los organismos públicos adscritos al Departamento y del nombramiento de personas delegadas adjuntas en todas las representaciones en el Exterior.

Artículo 11. *Estructura normativa de la seguridad de la información.*

1. El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se podrá estructurar como máximo en los siguientes niveles relacionados jerárquicamente:

a) Primer nivel normativo: PSI y directrices. Está constituido por la PSI y las directrices generales de seguridad aplicables a los órganos superiores o directivos del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, a los que, conforme al artículo 1, sea de aplicación esta PSI.

b) Segundo nivel normativo: Normativa y recomendaciones de seguridad. Está constituido por la normativa y recomendaciones de seguridad que se definan en cada ámbito organizativo de aplicación específico (órganos superiores y directivos, y organismos públicos dependientes a los que sea de aplicación esta PSI, conforme al artículo 1). La normativa, que comprende los procedimientos, las normas y las instrucciones técnicas de seguridad se formalizará mediante instrucciones o resoluciones de las personas titulares de los órganos correspondientes, previa aprobación en la Comisión Permanente de la CMAD, mientras que las recomendaciones consistirán en buenas prácticas y consejos no vinculantes para mejorar las condiciones de seguridad.

cve: BOE-A-2021-17277
Verificable en https://www.boe.es

c) Tercer nivel normativo: Procedimientos técnicos. Está constituido por el conjunto de procedimientos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. Son recomendaciones o informaciones relativas a temas concretos de seguridad basadas en Instrucciones previas, que establecen las configuraciones mínimas de seguridad de los diferentes elementos de un sistema de información, recomendaciones de uso o de otro tipo. La responsabilidad de aprobación de estos procedimientos técnicos recae en la persona responsable de seguridad. Se consideran incluidas en este nivel normativo las guías CCN-STIC elaboradas por el Centro Criptológico Nacional.

2. Además de la normativa enunciada en este artículo, la estructura normativa podrá disponer, a criterio de cada uno de los órganos u organismos adscritos a esta PSI, y siempre dentro del ámbito de sus competencias y responsabilidades, de otros documentos tales como: informes técnicos, registros, evidencias, entre otros.

Artículo 12. *Gestión de los riesgos.*

1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad y protección de datos, basada en los riesgos (artículo 6 del Real Decreto 3/2010, de 8 de enero, artículo 24 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre) y reevaluación periódica (artículo 9 del Real Decreto 3/2010, de 8 de enero), siendo la persona o unidad responsable del servicio la encargada de solicitar el preceptivo análisis de riesgos y de que se proponga el tratamiento adecuado, calculando los riesgos residuales. El responsable de seguridad, tras la calificación de la información y la determinación del nivel de seguridad del sistema, obtendrá la matriz de aplicabilidad y el conjunto de medidas para garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información y del servicio. Se realizará la evaluación de riesgo identificando los riesgos residuales y, determinando, sobre la base de estos, el Plan de Tratamiento de Riesgo, que será comunicado al responsable de la información y del servicio.

2. La persona o unidad responsable de seguridad es la persona encargada de realizar dicho análisis en tiempo y forma, a petición de la persona responsable de la información y/o de la persona responsable del servicio, así como de identificar carencias y debilidades y ponerlas en conocimiento de las personas responsables de la información y del servicio.

3. Las personas responsables de la información y del servicio son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

4. El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por la persona titular del órgano o unidad administrativa o, en su caso, organismo autónomo, a través de un Plan de Adecuación al Esquema Nacional de Seguridad.

5. En cumplimento del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021 de 30 de marzo, el nivel de seguridad en la identificación electrónica de los sistemas de información que soporten procedimientos o servicios donde sea requerida, se determinará sobre la base del análisis de riesgos, de acuerdo con el Esquema Nacional de Seguridad y normativa correspondiente.

6. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero y siguiendo las

cve: BOE-A-2021-17277
Verificable en https://www.boe.es

normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.

Artículo 13. *Protección de datos de carácter personal.*

Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, 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 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Además, en cumplimiento de la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, se aplicarán las medidas de seguridad correspondientes a la categoría del Sistema según el Anexo II 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. En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en el Anexo II del Real Decreto 3/2010 de 8 de enero, dichas medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos de carácter personal.

Asimismo, se aplicarán las medidas técnicas que pudieran derivar de las nuevas normas aplicables en materia de protección de datos que se puedan aprobar en el futuro.

Artículo 14. *Formación y concienciación en seguridad de la información.*

1. Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos del Departamento, así como a la difusión entre los mismos de la PSI y de su desarrollo normativo.

2. La CP-CMAD y los responsables de seguridad se encargarán de promover las actividades de formación y concienciación en materia de seguridad, según lo indicado en el artículo 6.2.g) y en el artículo 8.3.h).

Artículo 15. *Actualización permanente.*

La PSI regulada en esta orden deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de Administración Digital, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad, a cualquier tipo de normativa que afecte a la seguridad de la información y a las normas aplicables en materia de protección de datos.

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

Las medidas descritas en esta orden no supondrán incremento del gasto, de conformidad con el apartado uno de la disposición adicional trigésima cuarta de la Ley 11/2020, de 30 de diciembre, de Presupuestos Generales del Estado para el año 2021. Dichas medidas serán atendidas con los medios materiales y humanos de que dispone el Ministerio de Asuntos Exteriores, Unión Europea y Cooperación.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Orden AEC/1647/2013, de 5 de septiembre, por la que se aprobó la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Asuntos Exteriores y de Cooperación.

cve: BOE-A-2021-17277
Verificable en https://www.boe.es

Disposición final primera. *Modificación de la Orden AEC/1372/2016 de 19 de julio, por la que se crea y regula la Comisión Ministerial para la Administración Digital del Ministerio de Asuntos Exteriores y de Cooperación.*

La Orden AEC/1372/2016 de 19 de julio, por la que se crea y regula la Comisión Ministerial para la Administración Digital del Ministerio de Asuntos Exteriores y de Cooperación, queda modificada como sigue:

Uno. El apartado 2.i) del artículo 3 queda redactado del siguiente modo, eliminándose el apartado 2.j):

«i) Ejercer las funciones en el gobierno de la Seguridad de la Información establecidas por la Orden que establece la Política de Seguridad de la Información (PSI) en el ámbito de la administración digital del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, aparte de las que le son conferidas en esta orden.»

Dos. El apartado 5 del artículo 4 queda redactado del siguiente modo:

«5. La Comisión Permanente de la CMAD podrá crear un Grupo de Trabajo para la elaboración de la documentación y recabar la información pertinente para la toma de sus decisiones en materia de la Seguridad de la Información.»

Disposición final segunda. *Instrucciones de ejecución.*

La persona titular de la Subsecretaría del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación podrá dictar las instrucciones necesarias para el mejor cumplimiento de esta orden.

Disposición final tercera. *Publicidad de la PSI.*

Esta orden se publicará en la Sede electrónica asociada del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación, así como en las Sedes electrónicas de los órganos adscritos al mismo, que no tengan establecida su propia política de seguridad, y en cuyo ámbito sea de aplicación.

Disposición final cuarta. *Entrada en vigor.*

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

Madrid, 15 de octubre de 2021.–El Ministro de Asuntos Exteriores, Unión Europea y Cooperación, José Manuel Albares Bueno.

cve: BOE-A-2021-17277
Verificable en https://www.boe.es