III. OTRAS DISPOSICIONES

MINISTERIO DE CULTURA Y DEPORTE

440 *Orden CUD/1313/2019, de 27 de diciembre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica del Ministerio de Cultura y Deporte.*

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

En línea con el impulso hacia la digitalización de dicho marco, y con objeto de que las consolidadas relaciones digitales se popularicen, la Administración debe ser confiable, para que los ciudadanos realicen los trámites administrativos con total seguridad y fiabilidad. Esta confianza en los sistemas de información debe extenderse a las garantías no solo sobre las comunicaciones sino también sobre el tratamiento y almacenamiento de la información.

Para ello, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas. 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 tales como el robo de datos e información, el hackeo de dispositivos móviles y sistemas industriales, o los ciberataques contra infraestructuras críticas, que exigen una mejor protección de redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano.

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 Real Decreto 3/2010, de 8 de enero.

Por otra parte, la protección de las personas físicas en relación con el tratamiento de datos personales, es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, tiene por objeto garantizar estos derechos de la ciudadanía y adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus 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).

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 eficiencia, 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 Cultura y Deporte. 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 procurado la participación de las partes interesadas,

cve: BOE-A-2020-440
Verificable en https://www.boe.es

permitiendo una gestión más eficiente de los recursos públicos y no contempla cargas administrativas.

La presente orden ministerial ha sido informada por la Comisión Ministerial de Administración Digital del Ministerio de Cultura y Deporte y por la Agencia Española de Protección de Datos.

Esta orden se dicta en cumplimiento de lo requerido por el artículo 11 del Real Decreto 3/2010, de 8 de enero.

En su virtud, con la aprobación previa del Ministro de Política Territorial y Función Pública, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. Constituye el objeto de la presente orden la aprobación de la Política de Seguridad de la Información (en adelante PSI) en el ámbito de la administración electrónica del Ministerio de Cultura y Deporte, así como del marco organizativo y tecnológico de la misma.

2. La PSI será de obligado cumplimiento para todos los órganos superiores y directivos del Ministerio de Cultura y Deporte, incluidos los organismos dependientes o adscritos al mismo que no tengan establecida su propia política de seguridad, siendo aplicable a todos los activos empleados por el Departamento.

3. La PSI será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información que sea gestionada por el Departamento, con independencia de cuál sea su destino, adscripción o relación con el mismo.

Artículo 2. *Competencias del Departamento.*

El Ministerio de Cultura y Deporte es el Departamento de la Administración General del Estado encargado de la promoción, protección y difusión del patrimonio histórico español, de los museos estatales y de las artes, del libro, la lectura y la creación literaria, de las actividades cinematográficas y audiovisuales y de los archivos y bibliotecas estatales, de la promoción y difusión de la cultura en español, así como de la propuesta y ejecución de la política del Gobierno en materia de deporte. Asimismo, le corresponde a este Departamento el impulso de las acciones de cooperación cultural y, en coordinación con el Ministerio de Asuntos Exteriores, Unión Europea y de Cooperación, de las relaciones internacionales en materia de cultura.

Artículo 3. *Marco legal y regulatorio.*

El marco normativo en que se desarrollan las actividades del Ministerio de Cultura y Deporte, en el ámbito de la prestación de los servicios electrónicos a los ciudadanos, sin perjuicio de la legislación específica, se compone de:

1. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
2. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
3. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en al ámbito de la Administración Electrónica.
4. 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.
5. 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).
6. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

cve: BOE-A-2020-440
Verificable en https://www.boe.es

7. Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

8. Orden CUL/395/2010, de 17 de febrero, por la que se crea la Sede Electrónica del Ministerio de Cultura.

9. Resolución de 19 de febrero de 2010, de la Presidencia del Consejo Superior de Deportes, por la que se crea la Sede Electrónica del Consejo Superior de Deportes.

10. Orden CUL/3410/2009, de 14 de diciembre, por la que se regula el Registro Electrónico del Ministerio de Cultura.

11. Resolución de 24 de junio de 2009, de la Presidencia del Consejo Superior de Deportes, por la que se crea el registro electrónico del Consejo Superior de Deportes.

12. Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

13. Texto refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo 1/1996, de 12 de abril, y su normativa de desarrollo.

14. Orden CUD/458/2019, de 12 de abril, por la que se crea la Comisión Ministerial de Administración Digital del Ministerio de Cultura y Deporte y se regula su composición y funciones.

15. 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.

16. 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.

Del mismo modo, forman parte del marco regulatorio las normas aplicables a la Administración Electrónica del Departamento que desarrollen o complementen las anteriores y que se encuentren dentro del ámbito de aplicación de la PSI.

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.

b) Responsabilidad diferenciada: en los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios; y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.

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 a lo establecido en los artículos 24, 25 y 32 del Reglamento (UE) 2016/679, 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, por el que se regula el Esquema Nacional de Seguridad en al ámbito de la Administración

cve: BOE-A-2020-440
Verificable en https://www.boe.es

Electrónica, 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 desde el diseño y por defecto: los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

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:

a) Protección de datos personales: se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos. Tal y como se establece en el Reglamento (UE) 2016/679, y en Ley Orgánica 3/2018, de 5 de diciembre, dichas medidas deberán ser apropiadas en función del análisis de riesgos mencionado en el apartado 4.1 d) del presente artículo, así como de una evaluación de impacto relativa a 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.

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 dichos activos.

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.

cve: BOE-A-2020-440
Verificable en https://www.boe.es

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: Los empleados públicos que prestan servicio al departamento tienen el derecho y el deber de conocer y aplicar la presente 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.

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, la presente PSI se establecerá asimismo en base a 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.

Artículo 5. *Estructura organizativa.*

La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI del Ministerio de Cultura y Deporte está compuesta por los siguientes agentes:

1. La Comisión Ministerial de Administración Digital (en adelante CMAD).
2. El Responsable de Seguridad.
3. Los Responsables de la Información.
4. Los Responsables del Servicio.
5. Los Responsables del Sistema.
6. Los Delegados de Protección de Datos.

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

1. La Comisión Ministerial de Administración Digital (CMAD) es el órgano colegiado de ámbito departamental responsable del impulso y coordinación interna en materia de Administración Digital.

2. El pleno de la CMAD gestionará y coordinará todas las actividades relacionadas con la seguridad de los sistemas de información, de forma adicional al ejercicio de las funciones que le corresponden de acuerdo con el artículo 4 de la Orden CUD/458/2019, de 12 de abril, por la que se crea la Comisión Ministerial de Administración Digital del Ministerio de Cultura y Deporte y se regula su composición y funciones. En particular, ejercerá las siguientes funciones:

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) Aprobar las normas de desarrollo de la PSI de segundo nivel, según lo previsto en el artículo 11 de esta orden.

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

cve: BOE-A-2020-440
Verificable en https://www.boe.es

e) Resolver los posibles conflictos que puedan derivarse del establecimiento de la estructura organizativa de seguridad, así como aquellos conflictos de competencia que pudieran aparecer entre los diferentes centros directivos en materia de seguridad de la información.

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) Tomar aquellas decisiones que garanticen la seguridad de la información y de los servicios del Departamento, así como la evaluación y seguimiento de las decisiones tomadas para satisfacer los requisitos de seguridad de la información y de los servicios.

i) Apoyar la coordinación, cooperación y colaboración con otras Administraciones Públicas en materia de Seguridad de la Información a través de los órganos que se creen al respecto en las Administraciones Públicas.

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. El pleno de la CMAD podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

Artículo 7. *El Responsable de Seguridad.*

1. Conforme al artículo 10 del Esquema Nacional de Seguridad, el Responsable de Seguridad es quien determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

2. Las funciones del Responsable de Seguridad se ejercerán por el Grupo Técnico de Seguridad de la Información (en adelante GTSI), órgano colegiado que se adscribe la Subsecretaría, y que estará compuesto por los siguientes miembros:

a) Presidente: La persona titular de la Dirección de la División de Tecnologías de la Información. Tendrá voto de calidad en la toma de decisiones del Grupo. En caso de ausencia, vacante o enfermedad será sustituido por el Vicepresidente.

b) Vicepresidente. La persona titular de la Subdirección General Adjunta de la División de Tecnologías de la Información.

c) Vocales: La persona titular de la Jefatura de Área de Infraestructuras de la División de Tecnologías de la Información y un representante de cada uno de los organismos públicos adscritos a la presente política de seguridad, en el ámbito del Ministerio de Cultura y Deporte.

Los vocales representantes anteriormente indicados, así como sus sustitutos, serán designados por el titular de la Dirección del Organismo adscrito a la presente PSI. El sustituto del la persona titular de la Jefatura de Área de Infraestructuras de la División de Tecnologías de la Información será designado por la persona titular de dicha División.

d) Secretario: La persona titular de la Jefatura de Área de Infraestructuras de la División de Tecnologías de la Información, que tendrá voz y voto y que, sin perjuicio del resto de funciones que le corresponden, ejecutará las decisiones del Grupo, convocará sus reuniones y preparará los temas a tratar.

3. Serán funciones del Responsable de Seguridad y, por tanto, de dicho GTSI, las siguientes:

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

b) Elaborar la normativa de seguridad de segundo nivel definida en el artículo 11 de la presente orden y proponer su aprobación al Pleno de la CMAD.

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

cve: BOE-A-2020-440
Verificable en https://www.boe.es

d) 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.

e) Mantener un inventario actualizado de las normas de segundo nivel detalladas en el artículo 11 de la presente orden, con referencia a los responsables designados, así como a los informes de auditorías, autoevaluaciones y análisis de riesgos realizados y de las declaraciones y certificaciones de seguridad.

f) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución. Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.

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

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

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

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

k) Realizar los preceptivos análisis de riesgos y mantenerlos actualizados según la legislación vigente.

l) 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.

m) Realizar las tareas de coordinación y comunicación con el Responsable de Seguridad del Ministerio de Educación y Formación Profesional, así como con los Responsables de Seguridad de los demás Departamentos Ministeriales.

n) Cualesquiera otras funciones que el Real Decreto 3/2010, de 8 de enero, asigne a los responsables de seguridad.

4. Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el GTSI podrá designar los responsables de seguridad delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo.

5. A las reuniones del GTSI, podrán acudir representantes designados por los Delegados de Protección de Datos del departamento y de los organismos públicos dependientes, adscritos a la presente PSI. También podrán ser invitados puntualmente los Responsables de los Tratamientos de Datos Personales en el ámbito del departamento y de los organismos públicos adscritos. Puntualmente se podrá invitar a personal técnico propio o externo a las reuniones.

6. En el seno del GTSI, podrán crearse grupos de trabajo cuya función será la de apoyarlo en el ejercicio de sus funciones. Los grupos de trabajo tendrán la composición que, en cada caso, determine el GTSI.

7. El GTSI se reunirá con carácter ordinario con una periodicidad trimestral y con carácter extraordinario, cuando lo decida su Presidente. En cuanto a su funcionamiento, se regirá, en todo lo no previsto en la presente orden, por lo dispuesto en el Capítulo II, Sección 3.ª del Título Preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Artículo 8. *Los Responsables de la Información y los Responsables del Servicio.*

1. Los Responsables de la Información y los 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 Cultura y Deporte, así como los organismos dependientes o adscritos al mismo a los que, conforme al artículo 1, les

cve: BOE-A-2020-440
Verificable en https://www.boe.es

sea de aplicación la presente PSI, designarán estos responsables 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 7.3.e).

Artículo 9. *Los Responsables del Sistema.*

1. El Responsable del Sistema es quien tiene la responsabilidad de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

2. De conformidad con la disposición adicional cuarta del Real Decreto 817/2018, de 6 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Cultura y Deporte y se modifica el Real Decreto 595/2018, de 22 de junio, por el que se establece la estructura orgánica básica de los departamentos ministeriales, la División de Tecnologías de la Información 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 dependiente o adscrito al Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI, designará este responsable 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 7.3.e).

Artículo 10. *Los Delegados de Protección de Datos.*

1. El Delegado 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 y en el Capítulo III del Título V de la Ley Orgánica 3/2018, de 5 de diciembre. Tendrá en todo caso acceso al registro de las actividades de tratamiento de datos personales al que se refiere el artículo 30 del Reglamento (UE) 2016/679.

2. La designación de los Delegados de Protección de Datos del Ministerio de Cultura y Deporte y de los organismos dependientes o adscritos al mismo a los que, conforme al artículo 1, les sea de aplicación la presente PSI, se efectuará de conformidad con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre. En consecuencia, serán designados 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 tienen encomendadas. Se comunicarán los nombramientos al Responsable de Seguridad, para que pueda mantener el inventario mencionado en el artículo 7.3.e).

Artículo 11. *Estructura normativa.*

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 fundamentales de seguridad aplicables a los órganos superiores o directivos del Ministerio de Cultura y Deporte a los que, conforme al artículo 1, sea de aplicación la presente 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 la presente PSI), conforme al artículo 1. La normativa, que comprende los procedimientos, las normas y las instrucciones técnicas de seguridad, es de obligado cumplimiento y se formalizará mediante instrucciones o resoluciones de los titulares de los órganos correspondientes, previa aprobación del presidente del grupo técnico de seguridad de la información,

cve: BOE-A-2020-440
Verificable en https://www.boe.es

mientras que las recomendaciones consistirán en buenas prácticas y consejos no vinculantes para mejorar las condiciones de seguridad.

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 dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado. Se consideran incluidas en este nivel normativo las guías CCN-STIC elaboradas por el Centro Criptológico Nacional.

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

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, y artículo 24 del Reglamento (UE) 2016/679, 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 el Responsable del Servicio el encargado 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, en base a ellos, se determinará el Plan de Tratamiento de Riesgo, que le será comunicado al Responsable de la Información y del Servicio.

2. El Responsable de Seguridad es el encargado de realizar dicho análisis en tiempo y forma a petición del Responsable del Servicio, así como de identificar carencias y debilidades y ponerlas en conocimiento de los Responsables de la Información y del Servicio.

3. Los Responsables de la Información y del Servicio son los encargados 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 el titular del órgano o unidad administrativa o, en su caso, organismo adscrito, a través de un Plan de Adecuación al Esquema Nacional de Seguridad.

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

Artículo 13. *Protección de datos personales.*

Se aplicarán a los datos personales que sean objeto de tratamiento por parte del Ministerio de Cultura y Deporte las medidas de seguridad apropiadas derivadas del análisis de riesgos así como de las evaluaciones de impacto relativas a la protección de

cve: BOE-A-2020-440
Verificable en https://www.boe.es

datos, conforme se detalla en el Reglamento (UE) 2016/679 y en la Ley Orgánica 3/2018, de 5 de diciembre. Además, se aplicarán las medidas correspondientes al Anexo II del Real Decreto 3/2010, de 8 de enero. 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 personales.

Artículo 14. *Formación y concienciación.*

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 CMAD y el Responsable 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 7.3.i).

Artículo 15. *Actualización permanente.*

La PSI que se aprueba mediante la presente orden deberá mantenerse actualizada permanentemente para adecuarla al progreso de los servicios de Administración Electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

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

Las medidas descritas en esta orden no supondrán incremento del gasto, siendo atendidas con los medios materiales y humanos de que dispone el Ministerio de Cultura y Deporte.

Disposición adicional segunda. *Deber de colaboración en la implantación de la PSI.*

Todos los órganos y unidades del Departamento prestarán su colaboración en las actuaciones de implementación de la PSI aprobada por esta orden.

Disposición derogatoria única. *Derogación normativa.*

Se derogan cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente orden, y en particular, se considera parcialmente derogada la Orden ECD/298/2018, de 12 de marzo, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica del Ministerio de Educación, Cultura y Deporte, en todos aquellos aspectos que afecten al Ministerio de Cultura y Deporte o a sus organismos adscritos.

Disposición final primera. *Modificación de la Orden CUD/458/2019, de 12 de abril, por la que se crea la Comisión Ministerial de Administración Digital del Ministerio de Cultura y Deporte y se regula su composición y funciones.*

La Orden CUD/458/2019, de 12 de abril, por la que se crea la Comisión Ministerial de Administración Digital del Ministerio de Cultura y Deporte y se regula su composición y funciones, se modifica del modo siguiente:

Se añade una letra f) al artículo 2.1, con la siguiente redacción:

> «f) A las sesiones del Pleno se podrá invitar a los Delegados de Protección de Datos del Ministerio de Cultura y Deporte y de los organismos dependientes o adscritos al mismo a los que, conforme al artículo 1, les sea de aplicación la presente PSI, o persona a quien se designe por éstos, que actuarán con voz y sin voto».

cve: BOE-A-2020-440
Verificable en https://www.boe.es

Disposición final segunda. *Instrucciones de ejecución.*

Por parte del titular de la Subsecretaría de Cultura y Deporte se podrán dictar las instrucciones necesarias para el mejor cumplimiento de esta orden.

Disposición final tercera. *Entrada en vigor y publicidad de la PSI.*

1. La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».
2. Esta orden se publicará en las sedes electrónicas del Ministerio de Cultura y Deporte en cuyo ámbito sea de aplicación.

Madrid, 27 de diciembre de 2019.–El Ministro de Cultura y Deporte, José Guirao Cabrera.

cve: BOE-A-2020-440
Verificable en https://www.boe.es