III. OTRAS DISPOSICIONES

MINISTERIO DE CULTURA

16386 *Orden CLT/832/2024, de 29 de julio, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica del Ministerio de Cultura.*

El marco de relación entre la Administración Pública y los ciudadanos a través de los medios electrónicos se encuentra establecido en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, así como en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y en el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo.

En línea con el impulso hacia la digitalización de dicho marco, y con objeto de consolidar las relaciones digitales, 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 sobre las comunicaciones y al tratamiento y almacenamiento de la información.

Para ello, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, persigue reforzar la confianza en que los sistemas de información permitirán custodiar la información, 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 311/2022, de 3 de mayo.

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 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 Cultura. También se adecúa al principio de proporcionalidad, pues no existe otra alternativa menos restrictiva de derechos o que imponga más obligaciones y, en cuanto a los principios de seguridad jurídica, transparencia y eficiencia, la norma es coherente con el resto del ordenamiento

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

jurídico y se ha procurado la participación de las partes interesadas, 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 por la Agencia Española de Protección de Datos.

Esta orden se dicta en cumplimiento de lo requerido por el artículo 12 del Real Decreto 311/2022, de 3 de mayo.

En su virtud, con la aprobación previa del Ministro para la Transformación Digital y de la 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 Digital del Ministerio de Cultura, así como del marco organizativo y tecnológico de la misma, con los siguientes objetivos:

a) Garantizar el cumplimiento de la legislación vigente en materia de seguridad de la información.

b) Proteger los activos de información de amenazas internas y externas, garantizando la confidencialidad, integridad, autenticidad, trazabilidad y disponibilidad de la información generada y/o gestionada por la entidad.

c) Asegurar la disponibilidad de los servicios proporcionados por el Ministerio de Cultura, así como la capacidad de gestión de incidentes de seguridad de la información y el restablecimiento de los servicios críticos en caso de interrupción del funcionamiento habitual de los mismos o de desastre.

d) Promover una cultura de ciberseguridad a través de la concienciación y formación del personal.

2. La PSI será de obligado cumplimiento para todos los órganos superiores y directivos del Ministerio de Cultura, 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. *Misión y funciones de la organización.*

El Ministerio de Cultura, de acuerdo con lo establecido en el Real Decreto 323/2024, de 26 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Cultura, y se modifica el Real Decreto 1009/2023, de 5 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales, es el Departamento de la Administración General del Estado encargado de la propuesta y ejecución de la política del Gobierno en materia de 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. 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.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

Artículo 3. *Marco legal y regulatorio.*

1. El marco normativo en que se desarrollan las actividades del Ministerio de Cultura 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:

a) Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
b) Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
c) El Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo.
d) Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
e) 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).
f) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
g) 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.

2. Del mismo modo, forman parte del marco regulatorio sus normas de desarrollo, la norma por la que se desarrolla la estructura orgánica básica del Departamento, las normas aplicables a la Administración Digital en la Administración General del Estado y en el departamento que se encuentren en vigor en cada momento, las normas aplicables en materia de protección de datos y cualquier norma de ciberseguridad que resulte de aplicación.
3. El Grupo Técnico de Seguridad de la Información mantendrá un listado actualizado de la normativa aplicable.

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 las iniciativas estratégicas del Departamento para conformar un todo coherente y eficaz.
b) Responsabilidad diferenciada: en los sistemas de seguridad de la información se diferenciará el Responsable del Servicio y/o Información, el Responsable del Sistema y el Responsable de Seguridad de la Información. Asimismo, la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de esos sistemas.
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, aplicándose desde el diseño inicial de los sistemas de información.
d) Gestión de Riesgos: de acuerdo con lo establecido en la legislación vigente en materia de seguridad de la información y protección de datos personales, el análisis y

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

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 y adicionalmente siempre que se considere necesario, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario. La evaluación permanente del estado de seguridad deberá servir para medir la evolución del sistema de gestión de seguridad de la información, así como para detectar vulnerabilidades, deficiencias de configuración y actividades o comportamientos anómalos, y responder de manera oportuna.

g) Seguridad y privacidad desde el diseño y por defecto: se contemplarán los aspectos de seguridad y privacidad de la información en todas las fases del ciclo de vida de los sistemas de información y del tratamiento de datos, garantizando su seguridad y privacidad desde la fase de diseño y aplicando configuraciones de seguridad y privacidad por defecto que ofrezcan el máximo nivel de protección.

h) Prevención, reacción y recuperación: la seguridad del sistema de gestión de Seguridad de la Información deberá contemplar los aspectos de prevención, detección y respuesta necesarios para conseguir que las amenazas sobre el mismo no se materialicen y no afecten gravemente a la información que maneja, o los servicios que se prestan. Sin perjuicio de los demás principios básicos y requisitos mínimos de seguridad establecidos, el sistema deberá garantizar la conservación de los datos e informaciones en soporte electrónico. Se deberán aplicar medidas de detección orientadas a descubrir la presencia de un incidente de seguridad. Asimismo, se aplicarán medidas de respuesta, dirigidas a gestionar en tiempo oportuno, la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

i) Líneas de defensa: el sistema de gestión de Seguridad de la Información deberá contar con una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita ganar tiempo para una reacción adecuada frente a los incidentes, reducir la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto sobre el mismo. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

2. Principios particulares, requisitos mínimos, responsabilidades específicas y objetivos de seguridad.

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) Organización e implantación del proceso de seguridad: La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización. En los sistemas de información se diferenciará:

1.º El responsable de la información, que determinará los requisitos de seguridad de la información tratada.

2.º El responsable del servicio, que determinará los requisitos de seguridad de los servicios prestados.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

3.º El responsable del sistema, que se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo.

4.º El responsable de seguridad, que determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.

El responsable de la seguridad será preferiblemente distinto del responsable del sistema, y no existirá dependencia jerárquica entre ambos. En caso de existir justificadamente dependencia jerárquica entre ellos debido a la estructura de la organización, se aplicarán medidas compensatorias para garantizar la imparcialidad en sus actuaciones.

b) Gestión de personal: se implantarán los mecanismos necesarios para que cualquier persona con acceso a los sistemas de información del Ministerio, reciba formación e información acerca de sus deberes, obligaciones y responsabilidades en materia de seguridad de la información. El Ministerio se reserva el derecho de supervisar las actividades de los usuarios para verificar el cumplimiento tanto de la presente política como de la normativa y procedimientos de seguridad que la desarrollen. La monitorización de las actividades de los usuarios se realizará conforme a lo establecido por la legislación vigente que resulte de aplicación, así como por las normas, procedimientos e instrucciones técnicas desarrolladas por la organización.

c) Profesionalidad: la seguridad de la información será atendida, revisada y auditada por personal cualificado, diferenciado, dedicado e instruido en todas las fases del ciclo de vida de los sistemas de información. Dicho personal deberá cumplir con los requisitos de formación y experiencia exigidos por la organización para el desarrollo de los puestos de trabajo.

d) Autorización y control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información debidamente autorizados, y exclusivamente a las funciones permitidas. Para ello se implantarán 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.

e) Protección de las instalaciones: los activos de información serán emplazados en áreas seguras y protegidas por controles de acceso físicos adecuados a su nivel de criticidad y proporcionales en función de los análisis de riesgos, sin perjuicio de los requisitos de seguridad exigidos por la legislación vigente en lo que respecta a la protección de las infraestructuras críticas. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

f) Adquisición de productos de seguridad y contratación de servicios de seguridad: la selección de los productos y la contratación de los servicios de seguridad se deberá realizar teniendo en cuenta la categoría del sistema y el nivel de seguridad determinado, así como lo dispuesto por el principio de profesionalidad anteriormente indicado. Se deberán seleccionar aquellos productos y servicios que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, o bien, aquellos que cumplan con el criterio determinado por el Centro Criptológico Nacional, en caso de que no existan productos o servicios certificados.

g) Mínimo privilegio: los sistemas de información se diseñarán y configurarán aplicando los mínimos privilegios necesarios para su óptimo desempeño. Los sistemas proporcionarán las funcionalidades imprescindibles para que la organización pueda alcanzar sus objetivos competenciales o contractuales. Por tanto, las funciones de operación, administración y registro de actividad serán las mínimas necesarias y serán ejecutadas únicamente por el personal autorizado y empleando los medios o recursos habilitados para ello, pudiéndose exigir restricciones de horario y puntos de acceso facultados. La configuración de seguridad para las distintas tecnologías se aplicará

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

teniendo en cuenta la categoría del sistema, debiéndose eliminar y/o desactivar las funciones que resulten innecesarias o inadecuadas y aplicándose las guías de buenas prácticas de configuración segura. En todo caso, el uso habitual de los sistemas de información deberá ser siempre sencillo y seguro, de manera que el uso inseguro de estos requiera un acto consciente por parte de los usuarios.

h) Integridad y actualización del sistema: se requerirá de una autorización formal previa para la actualización del sistema, incluyendo la introducción o modificación de elementos físicos o lógicos en el inventario de activos del sistema.

i) Protección de la información almacenada y en tránsito: se aplicarán las medidas que se estimen necesarias para garantizar la seguridad de la información en tránsito o almacenada en cualquier soporte, debiéndose analizar previamente dicho soporte (equipos o dispositivos portátiles o móviles, dispositivos periféricos, papel, etc.) y las comunicaciones sobre redes abiertas, con el objeto de seleccionar las medidas más eficaces y garantizar de este modo una adecuada protección de la información. Además, se desarrollarán y aplicarán procedimientos que permitan alcanzar la recuperación y conservación a largo plazo, de los documentos electrónicos producidos por los sistemas de información. A la información almacenada en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica, se le aplicará las medidas que correspondan a la naturaleza del soporte, de conformidad con el ENS y las demás normas que resulten de aplicación.

j) Prevención ante otros sistemas de información interconectados: se aplicarán medidas de seguridad que permitan garantizar la protección del perímetro de los sistemas de información, debiéndose reforzar las actividades de prevención, detección y respuesta a incidentes de seguridad, principalmente, si se conectan a redes públicas, tal y como lo contempla la legislación especial en materia de Telecomunicaciones. Además, se deberán evaluar los riesgos derivados de la interconexión entre sistemas, controlándose su punto de unión y aplicando las recomendaciones realizadas en las instrucciones técnicas correspondientes.

k) Registro de la actividad y detección de código dañino: se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Estos registros se llevarán a cabo teniendo en cuenta el derecho al honor, a la intimidad y a la propia imagen, así como la legislación vigente en materia de protección de datos personales, función pública o laboral, y demás legislación aplicable. Además, con el propósito de garantizar la seguridad de la información, en caso necesario y de manera proporcional, se podrán analizar las comunicaciones entrantes o salientes, de modo que sea posible evitar el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio y evitar la distribución malintencionada de código dañino y/o de cualquier elemento que pueda afectar la seguridad de las redes y sistemas de información. Por otra parte, al objeto de corregir o, en su caso, exigir responsabilidades, cada usuario con acceso a los sistemas de información deberá estar identificado de forma única, debiendo quedar trazas en dichos sistemas, en todo momento, de quién recibe derechos de acceso, de qué tipo, y quién ha realizado una determinada actividad.

l) Gestión de los incidentes de seguridad: se implantarán los mecanismos apropiados para la correcta identificación, notificación, registro, análisis y resolución de los incidentes de seguridad. Se dispondrá de procedimientos de notificación y gestión de incidentes de seguridad de acuerdo con lo previsto en la legislación vigente y en las instrucciones técnicas de seguridad correspondientes. Estos procedimientos deberán ser conocidos y aplicados por todo el personal. Se mantendrá un registro de los incidentes que incluirá las medidas adoptadas para su resolución. Dichos registros se utilizarán para realizar las acciones de mejora continua que se consideren oportunas. Se colaborará con las entidades y autoridades de control en el reporte y cualquier acción que se considere en cuanto a incidentes de seguridad.

m) Gestión de la continuidad: se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información en caso de pérdida de los

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

medios habituales, así como para mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.

n) Clasificación de la información y gestión de activos de información: todos los activos de información se encontrarán inventariados, tendrán asignado un responsable y, en caso de ser necesario, un custodio. La información deberá ser clasificada y tratada en función de los niveles establecidos de acuerdo con su criticidad para la organización.

ñ) 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.

o) Gestión de proveedores: en caso de externalización de servicios, a los proveedores y personal externo o colaboradores, se les incluirá en el ámbito de esta PSI y de la normativa de Seguridad de la Información que la desarrolla. Cualquier cesión de datos deberá estar sujeta a los requisitos de seguridad establecidos tanto por la legislación vigente como por la normativa interna. Se deberán suscribir los acuerdos o contratos o compromisos que garanticen el cumplimiento de dichos requisitos. Además, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

p) 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 la legislación vigente en materia de protección de datos personales, dichas medidas deberán ser apropiadas en función del análisis de riesgos mencionado en el apartado 1 d), 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.

q) Cumplimiento: se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para garantizar el cumplimiento de la legislación vigente en materia de seguridad de la información, protección de datos personales, así como de la legislación especial que afecte al ámbito de actuación de la organización.

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 el Real Decreto 311/2022, de 3 de mayo.

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 está compuesta por los siguientes agentes:

1. Comisión Ministerial de Administración Digital.
2. Responsable de Seguridad.
3. Responsable de la Información.
4. Responsable del Servicio.
5. Responsable del Sistema.
6. Delegado de Protección de Datos.
7. Grupo de trabajo de delegados de Protección de Datos.
8. Comité de Crisis.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

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

1. La Comisión Ministerial de Administración Digital (en adelante CMAD) es el órgano colegiado responsable del impulso y coordinación interna del Departamento y sus organismos públicos en materia de Administración Digital.

2. La CMAD será establecida, y modificada, por Orden Ministerial.

3. Su estructura y composición, funcionamiento, ámbito de responsabilidad y relación con otros elementos de la organización están establecidos en 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, y posteriores modificaciones.

4. En cuanto a la seguridad de la información, 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. En particular, se encargará de:

a) Impulsar la seguridad de la información en la organización, aportando los recursos necesarios y apoyando a los distintos roles de seguridad de la información.

b) Aplicar, en el ámbito de actuación del Ministerio de Cultura, las directrices de seguridad establecidas por el ENS y demás legislación vigente en el ámbito de la seguridad de la información y las comunicaciones, así como supervisar su cumplimiento.

c) Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.

d) Elaborar las propuestas de modificación y actualización permanente de la PSI.

e) Velar e impulsar el cumplimiento de la PSI y de su desarrollo normativo.

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

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

h) Elevar informe a la máxima autoridad del Ministerio, sobre el estado de seguridad de la información.

i) Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

j) 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.

k) Gestionar y coordinar la implantación de las medidas de seguridad adoptadas.

l) Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

m) Promover la realización de las auditorías periódicas y autoevaluaciones de seguridad que permitan verificar el cumplimiento de las obligaciones del Ministerio en materia de seguridad.

n) 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 la PSI.

ñ) 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.

o) Aprobar planes de mejora de la seguridad de la información de la organización.

p) 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.

q) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la PSI y su normativa de desarrollo.

r) Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

Artículo 7. *El Responsable de Seguridad.*

1. 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 que ocupe el puesto de trabajo inmediatamente inferior a la dirección de la División de Tecnologías de la Información.

c) Vocales: Un representante de cada uno de los organismos públicos adscritos a la presente política de seguridad, en el ámbito del Ministerio de Cultura.

Los vocales representantes anteriormente indicados, así como sus sustitutos, serán designados por el titular de la Dirección del Organismo adscrito a la presente PSI.

d) Secretario: La persona titular de la Jefatura de Área de Comunicaciones y Seguridad de la Información de la División de Tecnologías de la Información o del Área equivalente, 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. En caso de ausencia o de que el puesto esté vacante, asumirá las funciones de Secretario del GTSI la persona que la División de Tecnologías de la Información designe como coordinador/a de la seguridad de la información.

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 16 y proponer su aprobación al Pleno de la CMAD.

c) Supervisar la efectividad de la normativa de seguridad desarrollada.

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

e) Impulsar el cumplimiento del cuerpo normativo definido en el artículo 16, así como velar por el mantenimiento de la documentación de seguridad y la gestión de mecanismos de acceso a la misma.

f) Mantener un inventario actualizado de las normas de segundo nivel detalladas en el artículo 16, 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.

g) Dirigir y coordinar la respuesta a los incidentes de seguridad, junto con los demás organismos y unidades del Ministerio.

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

i) Notificar los incidentes de seguridad a las autoridades competentes.

j) Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.

k) Compartir resultados del Informe Nacional del Estado de la Seguridad (INES) realizado anualmente por cada organismo en su ámbito correspondiente.

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

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

n) Impulsar la formación y concienciación en materia de seguridad de la información y apoyar a las áreas responsables de elaborar los planes de formación y

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

concienciación del Departamento, en el diseño y ejecución de dichos planes, con el objeto de garantizar que los mismos contemplan actividades formativas relacionadas a la seguridad de la información.

ñ) Promover la realización de análisis de riesgos, auditorías y controles periódicos, para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, por parte de las distintas áreas del Ministerio, así como para cumplir con los requisitos de seguridad exigidos por la legislación vigente.

o) 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.

p) Aprobar la declaración de aplicabilidad, que comprende la relación de las medidas de seguridad seleccionadas para los sistemas de información.

q) Realizar las tareas de coordinación y comunicación con los Responsables de Seguridad de los demás Departamentos Ministeriales.

r) Gestionar las revisiones externas o internas del sistema.

s) Gestionar los procesos de certificación.

t) Cualesquiera otras funciones que el Real Decreto 311/2022, de 3 de mayo, 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 mediante acuerdo y a propuesta de los vocales participantes de cada ámbito, podrá designar los Responsables de Seguridad delegados que considere necesarios, que gestionarán en su ámbito todas aquellas acciones que les delegue el mismo.

5. Teniendo en cuenta los asuntos a tratar por el GTSI, a las reuniones convocadas por dicho órgano colegiado podrán acudir, en calidad de invitados, los Delegados de Protección de Datos del departamento y de los organismos públicos dependientes, adscritos a la presente PSI, o bien, representantes designados por estos. También podrán ser invitados puntualmente los Responsables de los Tratamientos de Datos Personales en el ámbito del departamento y de los organismos públicos adscritos. Asimismo, 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.

Artículo 8. *Los Responsables de la Información.*

1. Los Responsables de la Información tienen por misión supervisar el uso que se realice de la información manejada dentro de su ámbito, así como de cualquier error o negligencia que desemboque en un incidente de seguridad que afecte a cualquiera de las dimensiones de seguridad relevantes, especialmente a la confidencialidad, la autenticidad y a la integridad. Los responsables de la información se encargarán de:

a) Asignar, documentar y aprobar los niveles de seguridad requeridos en cada dimensión para cada uno de los activos de información, pudiendo recabar la oportuna propuesta del Responsable de Seguridad y teniendo en cuenta las disposiciones establecidas por el Real Decreto 311/2022, de 3 de mayo.

b) Gestionar los niveles de riesgo que afecten a la información, en base al nivel de riesgo aceptable fijado por la organización, y aceptar los niveles de riesgo residual asumibles.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

c) Velar por el cumplimiento de la normativa establecida por la Comisión Superior Calificadora de Documentos Administrativos (CSCDA), en lo que respecta a la información que forma parte del patrimonio documental.

d) En coordinación con el Delegado de Protección de Datos, asegurarse de que a la información que contenga datos de carácter personal se le aplica las medidas de seguridad exigidas por la legislación vigente en esa materia.

2. Los órganos superiores o directivos del Ministerio de Cultura, así como los organismos dependientes o adscritos al mismo a los que, conforme al artículo 1, les sea de aplicación la presente PSI, designarán a los Responsables de la Información 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.f).

Artículo 9. *Los Responsables del Servicio.*

1. Los Responsables del Servicio se encargarán de supervisar el uso que se realice de los servicios prestados dentro de su ámbito, así como de cualquier error o negligencia que desemboque en un incidente de seguridad que afecte a cualquiera de las dimensiones de seguridad relevantes, especialmente a la disponibilidad.

2. A los Responsables del Servicio se les atribuyen las siguientes funciones:

a) Determinar, documentar y aprobar los niveles de seguridad de los servicios, pudiendo recabar la oportuna propuesta del Responsable de Seguridad.

b) Establecer los requisitos de disponibilidad del servicio y, por lo tanto, los requisitos de todos los activos (aplicaciones, servidores, comunicaciones, personal, etc.…) de los que depende el servicio.

c) Gestionar los niveles de riesgo que afecten al servicio, en base al nivel de riesgo aceptable fijado por la organización, y aceptar los niveles de riesgo residual asumibles.

3. Los órganos superiores o directivos del Ministerio de Cultura, así como los organismos dependientes o adscritos al mismo a los que, conforme al artículo 1, les sea de aplicación la presente PSI, designarán a los Responsables del Servicio, 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.f).

Artículo 10. *Los Responsables del Sistema.*

1. El Responsable del Sistema tiene por misión llevar a cabo una adecuada explotación de los sistemas de información del Ministerio de Cultura. Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad. Sus funciones son:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

b) Definir la topología y sistema de gestión del Sistema de Información, estableciendo los criterios de uso y los servicios disponibles en el mismo.

c) Acordar, en coordinación con la CMAD y el Responsable de Seguridad, la suspensión del manejo de ciertos activos de información y/o la prestación de ciertos servicios, en caso de detectar la existencia de deficiencias graves de seguridad.

d) Adoptar las medidas correctoras adecuadas derivadas de las auditorías y autoevaluaciones realizadas.

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

f) Elaborar los procedimientos operativos necesarios.

g) Prestar al Responsable de Seguridad asesoramiento para la determinación de la Categoría del Sistema.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

h) Elaborar los planes de continuidad y ejecutarlos tras su aprobación.
i) Planificar la implantación de las salvaguardas en el sistema.
j) Elaborar, en coordinación con el Responsable de Seguridad, los planes de mejora de la seguridad de los sistemas de información.
k) Ejecutar el plan de seguridad aprobado.
l) Llevar a cabo las funciones del administrador de la seguridad del sistema:

1.º La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
2.º La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
3.º Aprobar los cambios en la configuración vigente del Sistema de Información.
4.º Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
5.º Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
6.º Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
7.º Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

2. El correspondiente centro directivo del Ministerio de Cultura, así como los organismos dependientes o adscritos al mismo a los que, conforme al artículo 1, les sea de aplicación la presente PSI, designarán a los Responsables del Sistema entre los funcionarios de la unidad administrativa dependiente responsable de gestionar las tecnologías de la información de cada ámbito. Se comunicarán los nombramientos al Responsable de Seguridad, para que pueda mantener el inventario mencionado en el artículo 7.3.f).

Artículo 11. *Los Delegados de Protección de Datos.*

1. Los Delegados de Protección de Datos, dentro de su ámbito de actuación, ya sea el Ministerio o sus organismos dependientes o adscritos, se encargarán de:

a) Promover el cumplimiento de la normativa vigente en materia de protección de datos personales; y asesorar en el desarrollo, actualización y mejora continua del marco normativo interno del Departamento en esta materia.
b) Supervisar las actuaciones de protección de datos, incluyendo su implementación, desde el diseño y por defecto, la asignación de responsabilidades y que se realizan las auditorías correspondientes.
c) Promover la concienciación y la formación del personal que participa en las operaciones de tratamiento de datos personales.
d) Informar y asesorar a las unidades en la realización de análisis de riesgos, evaluaciones de impacto, auditorías y controles periódicos, para verificar el cumplimiento de las obligaciones en materia de protección de datos personales.
e) Informar regularmente a la persona titular del Ministerio/Organismo acerca del cumplimiento de la normativa de protección de datos personales, mediante una memoria anual.
f) Promover las buenas prácticas compartidas en el Grupo de trabajo de Delegados de Protección de Datos.
g) Cooperar con las autoridades de control y actuar como interlocutor del responsable del tratamiento ante las mismas, así como trasladar las notificaciones de brechas de seguridad en materia de protección de datos a la autoridad de control y a los interesados cuando proceda.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

h) Asesorar al responsable del tratamiento en caso de reclamación de los afectados ante la autoridad de control.

2. Las funciones de los Delegados de Protección de Datos se ejercerán con el apoyo del equipo técnico competente en materia de seguridad de la información y protección de datos.

3. La designación de los Delegados de Protección de Datos del Ministerio de Cultura y de los organismos dependientes o adscritos al mismo a los que les sea de aplicación la PSI, se efectuará de conformidad con lo dispuesto por la legislación vigente en materia de protección de datos. Se comunicarán los nombramientos al Responsable de Seguridad, para que pueda mantener el inventario mencionado en el artículo 7.3.f).

Artículo 12. *Grupo de Trabajo de Delegados de Protección de Datos.*

1. Se constituye el Grupo de Trabajo de los Delegados de Protección de Datos, compuesto por los Delegados de Protección de Datos (DPD en adelante) del Ministerio y de sus organismos dependientes o adscritos:

a) DPD de la Biblioteca Nacional de España.
b) DPD de la Gerencia de Infraestructuras y Equipamientos de Cultura.
c) DPD de del Instituto de la Cinematografía y de las Artes Audiovisuales.
d) DPD del Instituto Nacional de las Artes Escénicas y de la Música.
e) DPD del Museo Nacional Centro de Arte Reina Sofía.
f) DPD del Museo Nacional del Prado.

Asimismo, serán miembros del Grupo de Trabajo los DPD que puedan nombrarse en futuros organismos adscritos al Ministerio.

Podrán participar en el Grupo de Trabajo cuantos asesores, internos o externos, estimen necesarios los miembros del mismo.

2. El Grupo de Trabajo de los Delegados de Protección de Datos ejercerá las siguientes funciones:

a) Supervisar la normativa de seguridad del Ministerio en relación con el cumplimiento de lo dispuesto en la normativa de protección de datos, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.

b) Proponer buenas prácticas relativas al tratamiento de los datos personales, teniendo en cuenta la legislación vigente, así como el criterio, las guías e informes de la autoridad de control de protección de datos.

c) Cuando se considere oportuno, promover la unificación de metodologías, criterios y la documentación general a utilizar en materia de protección de datos.

d) Acordar respuestas coordinadas para corregir las desviaciones de las actuaciones relacionadas con la seguridad y el tratamiento de los datos personales identificadas por los miembros del Grupo de Trabajo.

3. Las funciones del Grupo de Trabajo de Protección de Datos se ejercerán con el apoyo del equipo técnico especializado en materia de seguridad de la información y protección de datos.

4. El Grupo de Trabajo de Delegados de Protección de Datos se reunirá, al menos, una vez al año y cuando se estime necesario a petición de alguno de sus miembros. 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.

5. Las labores de secretaría del grupo de trabajo se asumirán por un funcionario dependiente de la Subdirección General de Atención al Ciudadano, Documentación y Publicaciones, designado por el titular de la misma.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

Artículo 13. *Comité de Crisis.*

1. El Comité de Crisis es el órgano colegiado encargado de gestionar, tomar decisiones y coordinar las acciones necesarias para hacer frente o resolver la emergencia relacionada con la seguridad de la información que haya sido calificada como crisis.

Este Comité supervisará la recuperación de los sistemas de información considerados como críticos para el Ministerio de Cultura, en caso de desastres o incidentes graves.

2. El Comité de Crisis estará integrado por los siguientes miembros:

a) Presidente: La persona titular de la Subsecretaría de Cultura, quién ocupará el rol de Responsable de Gestión de la Crisis.

b) Vicepresidente: La persona titular del Gabinete Técnico de la Subsecretaría.

c) Vocales:

1.º La persona titular de la Dirección del Gabinete del Ministro.

2.º La persona titular de la Subdirección General de Recursos Humanos e Inspección de Servicios.

3.º La persona titular de la Subdirección General de Gestión Económica.

4.º La persona titular de la Subdirección General de Asuntos Generales.

5.º La persona titular de la Subdirección General de Atención al ciudadano, Documentación y Publicaciones.

6.º El Delegado de Protección de Datos en la organización.

7.º La persona titular de Jefatura de Área de Infraestructuras y Sistemas de la División de Tecnologías de la Información.

8.º La persona titular de Jefatura de Área de Comunicaciones y Seguridad de la Información de la División de Tecnologías de la Información.

9.º Un Representante de la Abogacía del Estado en el Departamento.

3. Secretario: La persona titular de la Dirección de la División de Tecnologías de la Información, que actuando en calidad de Presidente del GTSI –órgano colegiado que ejerce el rol de Responsable de Seguridad–, tendrá voz y voto y que, sin perjuicio del resto de funciones que le corresponden, ejecutará las decisiones del Comité, convocará sus reuniones y preparará los temas a tratar.

En casos de ausencia, vacante o enfermedad, los vocales titulares serán sustituidos por sus suplentes. Los suplentes serán designados por el titular de la unidad afectada.

4. Se podrán convocar en calidad de Vocal, a representantes de los distintos organismos dependientes o adscritos al Ministerio de Cultura, que guarden relación con la crisis o situación de emergencia.

5. El Comité de Crisis tendrá las siguientes funciones:

a) Detectar y prever acontecimientos que pudieran generar una situación de crisis y elaborar un plan de acción para evitar la materialización del hecho.

b) Identificar si un hecho o incidente se considera como una situación de crisis a través de la realización de estudios de situación y previsión de escenarios.

c) Establecer una estrategia que permita proteger la imagen pública y la reputación de la organización, ante el impacto que pudiera generar el incidente o la situación de crisis.

d) Llevar a cabo la gestión unificada de cualquier situación de crisis que surja en el Ministerio de Cultura.

e) Determinar la política informativa interna y externa durante la situación de crisis.

f) Actuar como centro de referencia de información durante la respuesta al incidente y su posterior recuperación, tanto ante los agentes internos como externos (Administración y otros) involucrados o concernidos por el incidente, asegurando de este modo las relaciones y la interlocución con todas las partes interesadas.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

g) Establecer responsabilidades a las distintas áreas del Ministerio, para facilitar la resolución de la situación que provoca la crisis y la coordinación entre dichas áreas.

h) Acelerar el proceso de toma de decisiones con el objetivo de hacer frente a incidentes o cualquier situación de crisis que surja en la organización, debiendo también establecer una estrategia y/o táctica a seguir para poder solventar la situación.

i) Para el desarrollo de estas funciones, el Ministerio desarrollará una Guía o Plan de Crisis.

j) Coordinar las acciones de vuelta a la normalidad y de análisis posterior al incidente.

Artículo 14. *Resolución de conflictos.*

En caso de conflicto entre los distintos roles de seguridad, será resuelto por el Pleno de la CMAD.

Artículo 15. *Procedimientos de asignación de roles y cobertura de vacantes.*

Los roles de seguridad serán revisados cada cuatro años. En el caso de que exista una vacante la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

El procedimiento de asignación de los roles de seguridad es el siguiente:

a) Los miembros y vocales de la CMAD de acuerdo con lo establecido en su Orden de creación.

b) Los órganos superiores o directivos del Ministerio de Cultura, así como los organismos dependientes o adscritos al mismo a los que les sea de aplicación la PSI, designarán a los Responsables del Servicio, de la Información y del Sistema, de acuerdo con su propia organización interna.

c) Mientras no exista una designación explícita de responsables del servicio y/o de responsables de la información para cada uno de los procedimientos administrativos y servicios del Ministerio de Cultura, así como de los organismos dependientes o adscritos al mismo a los que les sea de aplicación la presente PSI, se entenderá designado para ambas funciones el responsable de la unidad administrativa que tenga encomendada la instrucción de cada procedimiento o la gestión de cada servicio. Mientras no exista una designación explícita del responsable del sistema, se entenderá designado como tal el responsable de la unidad administrativa que gestione las tecnologías de la información en cada ámbito.

d) La composición del GTSI se establece en la presente orden ministerial. En el caso de los Responsables de Seguridad delegados, estos serán designados por cada unidad u organismo dependiente o adscrito, de acuerdo con su propia organización interna.

e) La designación del Delegado de Protección de Datos del Ministerio de Cultura se efectuará de conformidad con lo dispuesto por la legislación vigente en materia de protección de datos. Los Delegados de Protección de Datos de los organismos adscritos al Ministerio serán designados por cada unidad u organismo dependiente o adscrito, de acuerdo con su propia organización interna y de conformidad con lo dispuesto en la legislación vigente en materia de protección de datos.

f) La composición del Comité de Crisis y del Grupo de Trabajo de Delegados de Protección de Datos se establece en la presente orden ministerial.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

Artículo 16. *Estructura normativa.*

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

a) Primer nivel normativo: PSI y directrices. Está constituido por la PSI del Ministerio de Cultura. La presente orden ministerial se publicará en las sedes electrónicas asociadas del Ministerio de Cultura y sus Organismos Públicos dependientes o adscritos en cuyo ámbito sea de aplicación.

b) Segundo nivel normativo: Normativa y recomendaciones de seguridad de adaptación del marco normativo de seguridad, de obligado cumplimiento dentro de su ámbito. Su entrada en vigor se formalizará mediante instrucciones o resoluciones de los titulares de los órganos correspondientes, previa aprobación de la CMAD.

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. Este nivel incluye las 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.

d) Cuarto nivel: Informes, registros y evidencias electrónicas. Está constituido por los documentos o informes técnicos que recogen el resultado y las conclusiones de un estudio o de una evaluación, registros de actividad o alertas de seguridad, es decir, los documentos de carácter técnico que recogen amenazas y vulnerabilidades a sistemas de información.

2. El cuerpo normativo de seguridad se encontrará a disposición del personal de la organización, teniendo en cuenta los principios de mínimo privilegio y de necesidad de conocer y responsabilidad de compartir. Además, estará sujeto a revisiones periódicas para garantizar su actualización.

Artículo 17. *Gestión de los riesgos.*

1. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información, conforme a los principios de gestión de la seguridad y protección de datos, basada en los riesgos y al principio de vigilancia continua y reevaluación periódica, reconocidos por la legislación vigente en materia de seguridad de la información y protección de datos personales, 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 declaración 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, así como de la CMAD.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

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 validarse cada año por el titular del órgano o unidad administrativa o, en su caso, organismo dependiente o adscrito.

5. Los análisis de riesgos, así como su tratamiento, se realizarán también cuando se detecten incidentes de seguridad o se identifiquen cambios organizativos, metodológicos, legales o tecnológicos que pudieran suponer un incremento del riesgo al que se encuentren expuestos los activos.

6. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 311/2022, de 3 de mayo, y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación de este, elaboradas por el Centro Criptológico Nacional.

7. Con una periodicidad al menos anual, y siempre que se realicen modificaciones sustanciales en los sistemas de información, la CMAD aprobará la definición de las medidas de seguridad, las cuales se deberán reevaluar y actualizar, de modo que su eficacia esté adaptada a la constante evolución de los riesgos y sistemas de protección.

8. Los análisis de riesgos, desde un enfoque de privacidad, se realizarán según lo establecido en la normativa vigente en materia de protección de datos personales, debiéndose seguir también las indicaciones de la Agencia Española de Protección de Datos y demás autoridades competentes al respecto.

Artículo 18. *Protección de datos personales.*

Se aplicarán las medidas de seguridad apropiadas en función del análisis de riesgo y, evaluación de impacto de los datos personales objeto de tratamiento por parte del Ministerio de Cultura, en cumplimiento de lo dispuesto en el artículo 24 del Reglamento General de Protección de Datos. Además, se aplicarán las medidas correspondientes al anexo II del Real Decreto 311/2022, de 3 de mayo. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto relativos a la protección de datos, en caso de resultar agravadas respecto de las previstas en el Real Decreto 311/2022, de 3 de mayo.

Artículo 19. *Formación y concienciación.*

1. En aplicación del principio de seguridad como un proceso integral, se desarrollarán actividades formativas específicas orientadas a la concienciación y formación del personal que preste servicio en el Ministerio de Cultura, así como a la difusión entre los mismos de la PSI y de su desarrollo normativo, pudiendo, en algún caso, recabar la colaboración de entidades encargadas de coordinar las acciones de seguridad de la información en el sector público.

2. Asimismo, se prestará la máxima atención a la concienciación de las personas a las que, como consecuencia de la aplicación de esta política, se les asignen roles y responsabilidades en materia de seguridad de la información, así como de los responsables jerárquicos de estas, con el propósito de evitar que la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas constituyan fuentes de riesgo para la seguridad.

3. Las actividades formativas y de concienciación se incluirán en el plan de formación que desarrolle el Ministerio de Cultura.

4. 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 los artículos 6 y 7.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es

Artículo 20. *Actualización permanente.*

La PSI que se aprueba mediante la presente 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.

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.

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

Todos los órganos y unidades del Ministerio de Cultura 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 derogada la 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, todo ello respecto del ámbito de competencias del actual Ministerio de Cultura.

Disposición final primera. *Instrucciones de ejecución.*

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

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

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

Madrid, 29 de julio de 2024.–El Ministro de Cultura, Ernest Urtasun Domènech.

cve: BOE-A-2024-16386
Verificable en https://www.boe.es