III. OTRAS DISPOSICIONES

MINISTERIO DE JUSTICIA

15662 *Orden JUS/1293/2017, de 14 de diciembre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica.*

La Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos. Dichos medios deben asegurar la interoperabilidad y seguridad de los sistemas y soluciones adoptadas, garantizarán la protección de los datos de carácter personal y facilitarán preferentemente la prestación conjunta de servicios a los interesados. En este sentido, el artículo 156 de la citada Ley 40/2015, de 1 de octubre, regula el Esquema Nacional de Seguridad.

Por su parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge en su artículo 13 sobre derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

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, modificado parcialmente por el Real Decreto 951/2015, de 23 de octubre, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación, sus principios básicos y los requisitos mínimos que permitan una protección adecuada de la información.

El artículo 11 del citado Real Decreto 3/2010, de 8 de enero, exige que todos los órganos superiores de las Administraciones públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II de la propia norma (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica, y función diferenciada) y desarrollará una serie de requisitos mínimos consignados en el ya mencionado artículo 11.1.

La presente Orden, por tanto, tiene la finalidad de aprobar la Política de Seguridad de la Información del Ministerio de Justicia, así como establecer la estructura organizativa para definirla, implantarla y gestionarla.

En virtud de lo anterior y en cumplimiento del artículo 11 del Real Decreto 3/2010, de 8 de enero, una vez recabado informe de la Agencia Española de Protección de Datos, y de la Comisión Ministerial de Administración Digital del Departamento y con la aprobación previa del Ministro de Hacienda 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 Justicia, 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 Justicia, siendo aplicable a los activos empleados por el Departamento en la prestación de los servicios de la Administración Electrónica.

3. La PSI afectará a la información tratada por medios electrónicos y a la información en soporte papel que el Ministerio gestiona en el ámbito de sus competencias. La taxonomía de la información se define según las siguientes normas:

a) Tendrá carácter de información clasificada la que esté afectada por la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales.

cve: BOE-A-2017-15662
Verificable en http://www.boe.es

b) La información que contenga datos de carácter personal se verá afectada por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo mientras estén vigentes y por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y demás disposiciones reguladoras de la materia.

c) La información contenida en los sistemas de información en el ámbito de la administración electrónica queda regulada por 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.

d) La información producida, conservada o reunida, cualquiera que sea su soporte, susceptible de formar parte del patrimonio documental se verá afectada por el Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original.

e) La información de gestión interna es aquella que no se produce como resultado de la función administrativa, aunque sea necesario disponer de ella para el correcto desarrollo de las competencias del Ministerio, como copias o duplicados de documentos originales que estén localizados y en buen estado de conservación, borradores o primeras versiones de documentos, publicaciones oficiales, ejemplares de ediciones, catálogos y publicaciones comerciales, así como el resto de información de apoyo que gestione el Departamento. A efectos de seguridad, confidencialidad y deber de secreto profesional, la información de gestión interna podrá ser calificada como protegida.

4. Se podrán adscribir a la presente PSI aquellos organismos públicos dependientes del Ministerio de Justicia que no tengan establecida su propia política de seguridad y así lo soliciten.

5. 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. *Principios de la seguridad de la información.*

1. 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.

cve: BOE-A-2017-15662
Verificable en http://www.boe.es

d) Gestión de Riesgos: 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 establecerá 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. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

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 y dedicado.

g) Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

2. 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 de carácter personal: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

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.

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.

cve: BOE-A-2017-15662
Verificable en http://www.boe.es

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.

Artículo 3. *Estructura organizativa.*

1. La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI del Ministerio de Justicia está compuesta por los siguientes agentes:

a) El Comité de Dirección de Seguridad de la Información.
b) El Grupo de Trabajo Técnico de Seguridad de la Información.
c) Los Responsables de Seguridad.
d) Los Responsables de la Información.
e) Los Responsables del Servicio.
f) Los Responsables del Sistema.
g) El Delegado de la Protección de Datos de carácter personal.

2. La estructura organizativa será competente para mantener, actualizar y hacer cumplir, dentro del ámbito definido por la presente Orden, la PSI del Ministerio de Justicia.

Artículo 4. *El Comité de Dirección de Seguridad de la Información.*

1. Adscrito a la Subsecretaría, se crea el Comité de Dirección de Seguridad de la Información (en adelante CDSI), como órgano colegiado de los previstos en el artículo 20.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que gestionará y coordinará todas las actividades relacionadas con la seguridad de los sistemas de información.

2. El CDSI estará compuesto por los siguientes miembros:

a) Presidente: La persona titular de la Subsecretaría de Justicia. Tendrá voto de calidad en la toma de decisiones del Comité. En caso de ausencia, vacante o enfermedad será sustituido por el titular de la Secretaría General Técnica del Ministerio de Justicia.

b) Vocales: Un representante de cada uno de los siguientes órganos u organismos del Departamento:

i. Secretaría de Estado de Justicia.
ii. Subsecretaría.
iii. Abogacía General del Estado-Dirección del Servicio Jurídico del Estado.
iv. Secretaría General Técnica.
v. Un representante de cada uno de los organismos dependientes del Ministerio que decidan adscribirse al PSI.
vi. El Delegado de Protección de Datos.

Los vocales representantes anteriormente indicados serán designados por el titular de la Subsecretaría de Justicia, a propuesta del titular del órgano, centro directivo u organismo autónomo respectivo, entre funcionarios con nivel de subdirector general o asimilados.

En caso de vacante, ausencia o enfermedad y en general cuando concurra una causa justificada, los miembros del Comité podrán de ser sustituidos por suplentes de tales órganos que reúnan las mismas condiciones. Serán designados por el mismo procedimiento que los titulares.

c) Secretario: La persona titular de la División de Tecnologías de la Información y las Comunicaciones, que tendrá voz y voto y que ejecutará las decisiones del Comité, convocará sus reuniones y preparará los temas a tratar.

cve: BOE-A-2017-15662
Verificable en http://www.boe.es

El Presidente del Comité podrá autorizar la asistencia a las reuniones de expertos en las materias que se vayan a tratar, que tendrán el carácter de asesores, con voz pero sin voto.

3. El CDSI ejercerá las siguientes funciones:

a) Elaborar las propuestas de modificación y actualización permanente de la PSI del Ministerio de Justicia.

b) Impulsar el cumplimiento de la PSI y su desarrollo normativo.

c) Aprobar las normas de desarrollo de la PSI de segundo nivel, según lo previsto en el artículo 13 de esta Orden.

d) Velar por la difusión de la PSI, promoviendo actividades de concienciación y formación en materia de seguridad para el personal del Departamento.

e) 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.

f) Tomar aquellas decisiones que garanticen la seguridad de la información y de los servicios del Departamento.

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

h) Aprobar el Plan de Auditoría y el Plan de Formación propuestos por el Responsable de Seguridad.

i) Resolver los conflictos de competencia que pudieran aparecer entre los diferentes centros directivos en materia de seguridad de la información.

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.

k) Definir, dentro del marco establecido por la presente Orden, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a la segregación de tareas.

4. El CDSI se reunirá con carácter ordinario al menos una vez al año 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, ya citada, que regula el funcionamiento de los órganos colegiados de la Administración.

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

Artículo 5. *Grupo de Trabajo Técnico de Seguridad de la Información.*

1. Con la finalidad de conocer las cuestiones técnicas que deban abordarse en relación con la PSI y con el fin de asegurar la coordinación en materia de seguridad de la información con el conjunto del Departamento y con otras instancias de la Administración General del Estado, se crea en el seno de la CDSI, con carácter permanente, el Grupo de Trabajo Técnico de Seguridad de la Información (GTTSI, en adelante).

2. El GTTSI estará compuesto por el titular de la División de Tecnologías de la Información y las Comunicaciones, el titular de la Subdirección General de Nuevas Tecnologías de la Justicia, el Delegado de Protección de Datos y los responsables de Seguridad definidos en el artículo 6.

3. El GTTSI colaborará con el CDSI en las cuestiones que éste le encomiende y, de forma particular le corresponderá:

a) Elaborar estudios, análisis previos y propuestas de modificación y actualización de la PSI.

b) Elaborar estudios, análisis previos y propuestas sobre la normativa de seguridad de segundo y tercer nivel.

c) Analizar el cumplimiento de la PSI y de su desarrollo normativo.

d) Analizar las medidas de seguridad de la información y de los servicios electrónicos prestados por los sistemas de información.

e) Estudiar las actividades de concienciación y formación en materia de seguridad.

cve: BOE-A-2017-15662
Verificable en http://www.boe.es

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

g) Seguimiento de las medidas resultado del análisis y gestión de riesgos de los activos.

4. El GTTSI se reunirá con carácter ordinario con una frecuencia mínima de dos veces al año y, con carácter extraordinario, cuando lo decida el presidente del CDSI.

Artículo 6. *Los responsables de seguridad.*

1. El Responsable de Seguridad es la persona que toma las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

2. La Secretaría de Estado de Justicia, la Subsecretaría de Justicia, así como cada organismo público dependiente del Departamento a los que sea de aplicación la presente PSI designará un Responsable de Seguridad, sin que, de acuerdo con lo previsto en la disposición adicional primera de la presente Orden, implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

3. El ámbito de actuación de cada Responsable de Seguridad se limitará única y exclusivamente a los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean competencia y responsabilidad directa del órgano al que pertenezca dicho Responsable de Seguridad.

4. Serán funciones de cada Responsable de Seguridad, dentro del ámbito de actuación enunciado en el punto anterior, las siguientes:

a) Promover 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 14 de la presente orden.

c) Velar e impulsar el cumplimiento del cuerpo normativo definido en el artículo 14 de la presente orden.

d) Encargarse de que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.

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

f) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución y participar en la toma de decisiones en momentos de alerta.

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

h) Proponer la categoría del sistema según el procedimiento descrito en el anexo I del Real Decreto 3/2010, de 8 de enero y las medidas de seguridad que deben aplicarse de acuerdo con lo previsto en el anexo II del mismo real decreto.

i) Asumir las funciones explícitamente atribuidas a la figura del Responsable de Seguridad en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

Artículo 7. *Los responsables de la información.*

1. Los Responsables de la Información tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos, en materia de seguridad, de la información que manejan. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta las medidas de seguridad que corresponda implantar atendidos los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

2. Las funciones de Responsable de la Información recaerán en la persona titular del órgano o unidad administrativa que gestione cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestione sin que, de acuerdo con lo previsto en la disposición adicional

cve: BOE-A-2017-15662
Verificable en http://www.boe.es

primera de la presente Orden, implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

Artículo 8. *Los responsables del servicio.*

1. 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. Si estos servicios incluyen datos de carácter personal, además deberán tenerse en cuenta las medidas de seguridad que corresponda implantar atendidos los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

2. Las funciones de Responsable del Servicio recaerán en la persona titular del órgano o unidad administrativa que gestione cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades del servicio de todos los procedimientos que gestione sin que, de acuerdo con lo previsto en la disposición adicional primera de la presente Orden, implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

Artículo 9. *Los responsables del sistema.*

1. El Responsable del Sistema es la persona cuya responsabilidad es desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, así como elaborar la normativa de seguridad de tercer nivel definida en el artículo 13 de la presente orden.

2. Cada órgano superior o directivo del Ministerio de Justicia, así como cada organismo público dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI, designará este perfil de acuerdo con su propia organización interna, sin que, de acuerdo con lo previsto en la disposición adicional primera de la presente Orden, implique, en ningún caso, un aumento de las actuales dotaciones ni de las retribuciones de dichos efectivos por ningún concepto.

Artículo 10. *El Delegado de Protección de Datos.*

1. El Delegado de Protección de Datos será único para todos los órganos y organismos del Departamento y estará adscrito a la Subsecretaría del Ministerio de Justicia informándose de su nombramiento y cese a la Agencia Española de Protección de Datos.

2. Las funciones el Delegado de Protección de datos serán las indicadas en el ya mencionado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y demás disposiciones reguladoras de la materia.

Artículo 11. *Grupos de trabajo.*

Además del GTTSI, el CDSI podrá articular la creación de grupos de trabajo para la realización de actividades que se estimen convenientes, tales como la elaboración de estudios, trabajos e informes.

Artículo 12. *Resolución de conflictos.*

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la PSI prevalecerá la decisión del Comité de Dirección de Seguridad de la Información.

Artículo 13. *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 basada en los riesgos y reevaluación periódica. El Responsable del Servicio es el encargado de que se realice el

cve: BOE-A-2017-15662
Verificable en http://www.boe.es

preceptivo análisis de riesgos y se proponga el tratamiento adecuado, calculando los riesgos residuales.

2. Los Responsables de Seguridad, dentro de su ámbito de actuación, son los encargados de recomendar un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.

3. Los Responsables de la Información y del Servicio son los propietarios de los riesgos sobre la información y sobre los servicios, respectivamente, siendo responsables de su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

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

5. 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, así como todo lo referente al análisis de riesgo y de impacto en la protección de datos especificado en el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

Artículo 14. *Desarrollo normativo.*

1. El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: constituido por la PSI y las directrices generales de seguridad aplicables a los órganos superiores o directivos del Ministerio de Justicia a los que, conforme al artículo 1, sea de aplicación la presente PSI.

b) Segundo nivel normativo: constituido por las normas de seguridad desarrolladas por cada órgano superior o directivo del Ministerio de Justicia así como por cada organismo público dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI. Estas normas de seguridad deberán cumplir los siguientes requisitos:

i. Limitarse única y exclusivamente al ámbito específico de las competencias de cada uno de dichos órganos u organismos adscritos a la presente PSI. Este ámbito vendrá determinado por los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean prestados y gestionados directamente por dicho órgano u organismo.

ii. Cumplir estrictamente con lo indicado en el ENS y con el primer nivel normativo enunciado en el presente artículo.

iii. Ser aprobadas dentro del ámbito de cada uno de los citados órganos u organismos adscritos a la presente PSI.

c) Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la PSI, determinan las acciones o tareas a realizar en el desempeño de un proceso. Este tercer nivel normativo deberá cumplir los siguientes requisitos:

i. Limitarse única y exclusivamente al ámbito específico de las competencias de cada uno de dichos órganos u organismos adscritos a la presente PSI. Este ámbito vendrá determinado por los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean prestados y gestionados directamente por dicho órgano u organismo.

ii. Cumplir estrictamente con lo indicado en el ENS y con el primer y segundo nivel normativos enunciados en el presente artículo.

cve: BOE-A-2017-15662
Verificable en http://www.boe.es

iii. Ser aprobado dentro del ámbito de cada uno de los citados órganos u organismos adscritos a la presente PSI.

2. Además de la normativa enunciada en el apartado 1 del 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 estándares de seguridad, buenas prácticas o informes técnicos.

3. El personal de cada uno de los órganos u organismos adscritos a la presente PSI tendrá la obligación de conocer y cumplir, además de la presente PSI, todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones.

4. El CDSI establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en la medida de lo posible, en todo el ámbito de aplicación de la PSI.

5. Este marco normativo estará a disposición de todos los miembros del Ministerio de Justicia.

Artículo 15. *Protección de datos de carácter personal.*

1. En lo referente a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Justicia, se adoptarán las medidas técnicas y organizativas que corresponda implantar atendidos los riesgos generados por el tratamiento una vez llevada a cabo la evaluación exigida por el artículo 24.1 del Reglamento (UE) 2016/679.

2. Respecto a la protección de datos de carácter personal, el Responsable del Servicio asumirá las funciones de responsable del tratamiento.

3. En caso de conflicto entre los diferentes responsables, prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

Artículo 16. *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. El GTTSI se encargará de promover las actividades de formación y concienciación en materia de seguridad, según lo indicado en el artículo 5, apartado 3, letra e) de esta Orden.

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

La aplicación de esta orden no conllevará incremento del gasto público. Las medidas incluidas en la presente orden no supondrán incremento de dotaciones ni de retribuciones ni de otros gastos de personal.

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 adicional tercera. *Publicidad.*

Esta Orden se publicará en las sedes electrónicas del Ministerio de Justicia en cuyo ámbito sea de aplicación.

Disposición final única. *Entrada en vigor.*

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

Madrid, 14 de diciembre de 2017.–El Ministro de Justicia, Rafael Catalá Polo.

cve: BOE-A-2017-15662
Verificable en http://www.boe.es