III. OTRAS DISPOSICIONES

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

10965 *Orden HAP/1953/2014, de 15 de octubre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Hacienda y Administraciones Públicas.*

El marco de relación entre la Administración Pública y los ciudadanos a través de los medios electrónicos se encuentra establecido mediante la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Dicho marco de relación se establece a través de la Administración Electrónica, compuesta principalmente tanto por los sistemas de tecnologías de la información y comunicaciones destinados a este fin, como por el tratamiento y almacenamiento automatizado de la información que reside en los mismos.

La Administración Electrónica debe ser confiable para que los ciudadanos realicen los trámites administrativos correspondientes a través de la misma con total seguridad y fiabilidad. Para ello, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS) en el ámbito de la Administración Electrónica, determinado por el artículo 42 de la Ley 11/2007, de 22 de junio, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

La Política de Seguridad de la Información constituye el marco de referencia orientado a facilitar la definición, gestión, administración e implementación de los mecanismos y procedimientos de seguridad establecidos en el Real Decreto 3/2010, de 8 de enero.

Del mismo modo, determina que la Política de Seguridad de la Información debe ser coherente con lo establecido en el Documento de Seguridad que exige el artículo 88 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, en lo que corresponda, prevaleciendo lo relativo a la protección de datos de carácter personal en caso de discrepancias.

Esta orden ministerial ha sido informada por la Comisión Ministerial de Administración Electrónica y por el Consejo Superior de Administración Electrónica.

En su virtud, 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 Hacienda y Administraciones Públicas, 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 Hacienda y Administraciones Públicas, incluidos los órganos territoriales adscritos al mismo, que no tengan establecida su propia política de seguridad, siendo aplicable a los activos empleados por el Departamento en la prestación de los servicios de la Administración Electrónica.

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

cve: BOE-A-2014-10965

4. 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 del Departamento.*

El Ministerio de Hacienda y Administraciones Públicas es el Departamento de la Administración General del Estado encargado de la propuesta y ejecución de la política del Gobierno en las siguientes materias: Hacienda pública, presupuestos y gastos, empresas públicas, gestión de los sistemas de financiación y cooperación con la Administración autonómica y local, apoyo a las delegaciones y subdelegaciones del Gobierno, función pública, empleo público, formación de empleados públicos, de reforma y organización de la Administración General del Estado, procedimientos e inspección de servicios, impulso de la Administración Electrónica, evaluación de políticas públicas y mejora de la gestión pública y la calidad de los servicios.

Artículo 3. *Marco legal y regulatorio.*

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

1. Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
2. Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
3. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en al ámbito de la Administración Electrónica.
4. Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en al ámbito de la Administración Electrónica.
5. Ley Orgánica 15/1999 de diciembre, de 13 de diciembre, de Protección de Datos de Carácter Personal.
6. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
7. Ley 59/2003, de 19 de diciembre, de firma electrónica.
8. Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
9. Orden HAP/548/2013, de 2 de abril, por la que se crean y regulan sedes electrónicas en el Ministerio de Hacienda y Administraciones Públicas.
10. Orden HAP/547/2013, de 2 de abril, por la que se crea y se regula el Registro Electrónico del Ministerio de Hacienda y Administraciones Públicas.
11. Texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, y su normativa de desarrollo.

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

cve: BOE-A-2014-10965

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

1. Principios básicos.

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

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

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

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

d) Gestión de Riesgos: 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.

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. Principios particulares y responsabilidades específicas.

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

a) Protección de datos de carácter personal: se adoptarán las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.

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.

cve: BOE-A-2014-10965

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

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

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

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

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

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

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

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 Hacienda y Administraciones Públicas está compuesta por los siguientes agentes:

1. El Comité de Dirección de Seguridad de la Información.
2. El Grupo de trabajo Técnico de Seguridad de la Información.
3. Los Responsables de Seguridad.
4. Los Responsables de la Información.
5. Los Responsables del Servicio.
6. Los Responsables del Sistema.

Artículo 6. *El Comité de Dirección de Seguridad de la Información.*

1. Se crea el Comité de Dirección de Seguridad de la Información (en adelante CDSI), adscrito a la Subsecretaría del Ministerio de Hacienda y Administraciones Públicas. El CDSI estará compuesto por los siguientes miembros:

a) Presidente: El titular de la Subsecretaría del Ministerio de Hacienda y Administraciones Públicas.

b) Vicepresidente Primero: El titular de la Inspección General del Ministerio de Hacienda y Administraciones Públicas.

c) Vicepresidente Segundo: El titular de la Subdirección General de Servicios y Coordinación Territorial.

cve: BOE-A-2014-10965

d) Vocales:

i) Dos representantes de la Secretaría de Estado de Hacienda, nombrados por el titular de dicho órgano superior.
ii) Dos representantes de la Secretaría de Estado de Presupuestos y Gastos, nombrados por el titular de dicho órgano superior.
iii) Dos representantes de la Secretaría de Estado de Administraciones Públicas, nombrados por el titular de dicho órgano superior.
iv) El titular de la Subdirección General de Tecnologías de la Información y de las Comunicaciones, que actuará como Secretario.

2. El CDSI ejercerá las siguientes funciones:

a) Aprobar las propuestas de modificación y actualización permanente que se hagan sobre la PSI.
b) Aprobar el resto de la normativa de seguridad de primer nivel definida en el artículo 13.
c) Velar e impulsar el cumplimiento de la PSI y de su desarrollo normativo.
d) Promover la mejora continua en la gestión de la seguridad de la información.
e) Resolver los posibles conflictos que puedan derivarse del establecimiento de la citada estructura organizativa.

3. El CDSI se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida su Presidente.
4. El CDSI podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

Artículo 7. *Grupo de trabajo Técnico de Seguridad de la Información.*

1. Con carácter permanente se crea en el seno de la CDSI el «Grupo de Trabajo Técnico de Seguridad de la Información» (GTTSI en adelante) competente para conocer las cuestiones técnicas que deban de abordarse en relación con la PSI.
2. El GTTSI estará compuesto por los siguientes miembros: el titular de la Subdirección General de Tecnologías de la Información y de las Comunicaciones, un Inspector de los Servicios y los responsables de Seguridad definidos en el artículo 8. Asimismo, y con el fin de asegurar la coordinación en materia de seguridad de la información con el conjunto del Ministerio y con otras instancias de la AGE, el GTTSI contará con la participación del responsable de seguridad de la Agencia Estatal de la Administración Tributaria y podrán participar en el mismo representantes de órganos superiores o directivos del Ministerio de Hacienda y Administraciones Públicas y organismos públicos dependientes del Departamento a los que no les sea de aplicación la PSI.
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 para el resto de la normativa de seguridad de primer nivel definida en el artículo 13.
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.

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

cve: BOE-A-2014-10965

Artículo 8. *Los Responsables de Seguridad.*

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

Cada órgano superior o directivo del Ministerio de Hacienda y Administraciones Públicas 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.

2. 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 centro al que pertenezca dicho Responsable de Seguridad.

3. 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 y tercer nivel definida en el artículo 13.

c) Velar e impulsar el cumplimiento del cuerpo normativo definido en el artículo 13.

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

Artículo 9. *Los Responsables de la Información y los Responsables del Servicio.*

1. Los Responsables de la Información y los Responsables del Servicio tienen la potestad, dentro de su ámbito de actuación y de sus competencias, de establecer los requisitos, en materia de seguridad, de los servicios y de la información que manejan. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.

2. Cada órgano superior o directivo del Ministerio de Hacienda y Administraciones Públicas así como cada organismo público dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI, designará estos perfiles 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. *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.

2. Cada órgano superior o directivo del Ministerio de Hacienda y Administraciones Públicas 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 11. *Grupos de trabajo.*

El CDSI podrá articular la creación de grupos de trabajo para la realización de actividades tales como: estudios, trabajos e informes, que se estimen convenientes.

cve: BOE-A-2014-10965

Artículo 12. *Gestión de los riesgos.*

1. La gestión de riesgos debe realizarse de manera continua sobre los sistemas de información y contemplar un análisis de riesgos avanzado que evalúe los riesgos residuales y proponga tratamientos adecuados.

2. Cada órgano superior o directivo del Ministerio de Hacienda y Administraciones Públicas así como cada organismo público dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI, y siempre dentro de su ámbito de actuación y de sus competencias, se encargará de analizar y evaluar los riesgos de funcionamiento de los servicios a fin de establecer las correspondientes medidas preventivas.

3. Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y en especial las guías elaboradas por el Centro Criptológico Nacional.

Artículo 13. *Estructura normativa.*

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

a) Primer nivel normativo: constituido por la PSI y las directrices generales de seguridad aplicables a los órganos superiores o directivos del Ministerio de Hacienda y Administraciones Públicas 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 Hacienda y Administraciones Públicas 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:

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: 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:

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.

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

d) 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, informes técnicos, etc.

cve: BOE-A-2014-10965

e) 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.

Artículo 14. *Protección de datos de carácter personal.*

Se aplicarán a los datos de carácter personal que sean objeto de tratamiento por parte del Ministerio de Hacienda y Administraciones Públicas las medidas de seguridad determinadas en las siguientes normativas:

1. Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
2. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
3. Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Artículo 15. *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 Grupo de trabajo técnico de Seguridad de la Información y los Responsables de Seguridad se encargarán de promover las actividades de formación y concienciación en materia de seguridad, según lo indicado en el artículo 7, apartado 2, letra e y en el artículo 8, apartado 3, letra f de esta Orden.

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 Hacienda y Administraciones Públicas.

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 final única. *Publicidad de la PSI y entrada en vigor.*

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

Madrid, 15 de octubre de 2014.–El Ministro de Hacienda y Administraciones Públicas, Cristóbal Montoro Romero.

cve: BOE-A-2014-10965