III. OTRAS DISPOSICIONES

MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD

2378 *Orden SSI/321/2014, de 26 de febrero, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Sanidad, Servicios Sociales e Igualdad.*

El desarrollo de la Administración Electrónica implica el tratamiento automatizado de grandes cantidades de información por los sistemas de tecnologías de la información y de las comunicaciones, que está sometida a diferentes tipos de amenazas y vulnerabilidades.

En el contexto de la Administración Electrónica, se entiende por seguridad de la información la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes y acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de los datos almacenados o transmitidos y de los servicios que dichas redes o sistemas ofrecen, o a través de los cuales se realiza el acceso.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

La Política de Seguridad de la Información del Ministerio de Sanidad, Servicios Sociales e Igualdad, de conformidad con lo dispuesto en el artículo 11 del Real Decreto 3/2010, de 8 de enero, da soporte a todas las exigencias del Esquema Nacional de Seguridad, así como a los requisitos derivados de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su Reglamento de desarrollo, aprobado mediante el Real Decreto 1720/2007, de 21 de diciembre.

Dado que la seguridad de la información debe responder a múltiples requisitos y abarca todos los aspectos de una organización, es fundamental abordar su gestión utilizando un Sistema de Gestión de la Seguridad de la Información basado en el estándar UNE-ISO/IEC 27001. Las directrices para el establecimiento de un marco de control de la seguridad de la información que se incluyen en el Anexo se estructuran de acuerdo al estándar UNE-ISO/IEC 27002, para facilitar la implantación del Sistema de Gestión y para utilizar una estructura con independencia de las diferentes legislaciones vigentes.

Esta norma ha sido sometida a informe previo de la Agencia Española de Protección de Datos.

En su virtud, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. El objeto de esta orden es la aprobación de la Política de Seguridad de la Información (en adelante, PSI) en el ámbito de la Administración Electrónica del Ministerio de Sanidad, Servicios Sociales e Igualdad, así como el establecimiento del marco organizativo y tecnológico de la misma.

2. La PSI se aplicará a todos los sistemas de información utilizados por todos los órganos y unidades centrales y territoriales del Ministerio de Sanidad, Servicios Sociales e Igualdad y por los organismos públicos que dependan del mismo. La PSI deberá ser observada, igualmente, por todo el personal destinado en dichos órganos y unidades, así como por aquellas personas que, aunque no estén destinadas en los mismos, tengan acceso a sus sistemas de información.

cve: BOE-A-2014-2378

Artículo 2. *Misión del Departamento.*

Corresponde al Ministerio de Sanidad, Servicios Sociales e Igualdad la política del Gobierno en materia de salud, de planificación y asistencia sanitaria y de consumo, así como el ejercicio de las competencias de la Administración General del Estado para asegurar a los ciudadanos el derecho a la protección de la salud.

Asimismo, le corresponde la propuesta y ejecución de la política del Gobierno en materia de cohesión e inclusión social, de familia, de protección del menor y de atención a las personas dependientes o con discapacidad.

También le corresponden las políticas del Gobierno en materia de igualdad, lucha contra toda clase de discriminación y contra la violencia de género.

Artículo 3. *Marco normativo.*

1. El marco normativo en que se desarrollan las actividades del Ministerio de Sanidad, Servicios Sociales e Igualdad comprende la legislación sectorial reguladora de la actuación de los órganos superiores y directivos del Departamento y de los organismos públicos dependientes del mismo, así como la legislación específica en vigor sobre la administración electrónica que se detalla a continuación:

a) La legislación sectorial reguladora de la actuación de los órganos superiores y directivos del Ministerio de Sanidad, Servicios Sociales e Igualdad y de los organismos públicos dependientes, así como el Real Decreto 200/2012, de 23 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, Servicios Sociales e Igualdad y se modifica el Real Decreto 1887/2011, de 30 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales

b) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

c) 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.

d) 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.

e) Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

f) Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

g) 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.

h) Ley 59/2003, de 19 de diciembre, de firma electrónica.

i) Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

j) Orden SSI/2076/2013, de 28 de octubre, por la que se crea la sede electrónica del Ministerio de Sanidad, Servicios Sociales e Igualdad, así como las otras normas que hayan creado o puedan crear otras sedes electrónicas dentro del ámbito de aplicación de la PSI.

k) Orden SCO/2751/2006, de 31 de agosto, por la que se crea el Registro Telemático del Ministerio de Sanidad y Consumo para la presentación de escritos, solicitudes y comunicaciones y se establecen los requisitos generales para la tramitación telemática de determinados procedimientos, así como las otras normas que hayan creado o puedan crear otros registros electrónicos dentro del ámbito de aplicación de la PSI.

l) Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

2. También formarán parte de este marco normativo las restantes normas aplicables a la administración electrónica del Ministerio de Sanidad, Servicios sociales e Igualdad

cve: BOE-A-2014-2378

derivadas de las anteriores y que se encuentren publicadas en las sedes electrónicas comprendidas dentro del ámbito de la PSI.

Artículo 4. *Estructura organizativa de la PSI.*

La estructura organizativa de la gestión de la seguridad de la información en el ámbito de la administración electrónica del Ministerio de Sanidad, Servicios Sociales e Igualdad está compuesta por los siguientes agentes:

a) El Comité de Seguridad de la Información.
b) Los Responsables de Seguridad de la Información.
c) Los Responsables de la Información.
d) Los Responsables de los Servicios.

Artículo 5. *El Comité de Seguridad de la Información.*

1. Se crea el Comité de Seguridad de la Información (en adelante, Comité) como grupo de trabajo en el seno de la Comisión Ministerial de Informática del Departamento.
2. El Comité estará compuesto por los siguientes miembros:

a) Presidente: la persona titular de la Subsecretaría de Sanidad, Servicios Sociales e Igualdad.
b) Vicepresidente: la persona titular de la Subdirección General de Tecnologías de la Información
c) Vocales: un representante, con rango mínimo de Subdirector General o asimilado, de cada uno de los siguientes órganos superiores y directivos del Departamento:

1.º Secretaría de Estado de Servicios Sociales e Igualdad.
2.º Secretaría General de Sanidad y Consumo.
3.º Subsecretaría de Sanidad, Servicios Sociales e Igualdad.

Además serán vocales los Responsables de Seguridad de la Información del Instituto de Mayores y Servicios Sociales (IMSERSO), de la Organización Nacional de Trasplantes (ONT) y de los Centros de Ceuta y Melilla del Instituto Nacional de Gestión Sanitaria (INGESA).

d) Secretario: Con voz y sin voto, el Secretario del grupo técnico del Responsable de Seguridad de la Información del Ministerio de Sanidad, Servicios Sociales e Igualdad, que ejecutará las decisiones del Comité, efectuará la convocatoria de sus reuniones y preparará los temas a tratar.

3. El Comité coordinará todas las actividades relacionadas con la seguridad de los sistemas de información y ejercerá las siguientes funciones:

a) Elaborar las propuestas de modificación y actualización permanente de la PSI del Ministerio de Sanidad, Servicios Sociales e Igualdad con carácter anual.
b) Elaborar las propuestas de modificaciones en la estructura organizativa de la PSI del Ministerio de Sanidad, Servicios Sociales e Igualdad.
c) Determinar los criterios para la aceptación de riesgos y los niveles aceptables de riesgo para la organización.
d) Elaborar y aprobar la normativa de seguridad derivada de segundo nivel (normas de Seguridad de la Información) y el procedimiento de Análisis de Riesgos.
e) Proveer los recursos y medios necesarios para asegurar la concienciación y formación en materia de seguridad de la información de todo el personal del Ministerio de Sanidad, Servicios Sociales e Igualdad.
f) Compartir experiencias en materia de seguridad entre sus miembros para velar por el cumplimiento de la PSI y su normativa de desarrollo.
g) Analizar los Informes de Revisión por Dirección anuales facilitados por cada Responsable de Seguridad, en los que cada uno de ellos informará del resultado del

cve: BOE-A-2014-2378

análisis de riesgos, de las auditorías realizadas, del plan de proyectos y de las iniciativas y acciones de mejora de seguridad requeridas.

h) Revisar la información facilitada por los Responsables de Seguridad relativas a los incidentes de seguridad en el Ministerio de Sanidad, Servicios Sociales e Igualdad que así lo requieran.

i) Coordinar la actividad de los Responsables de Seguridad de cada dominio de seguridad para lograr una mayor eficacia.

j) Tomar todas aquellas decisiones que garanticen la seguridad de la información y servicios del Departamento.

4. El Comité se reunirá, al menos, una vez al año.

Artículo 6. *El Responsable de Seguridad de la Información.*

1. El Responsable de Seguridad de la Información (RSI) determina, en cada dominio de seguridad en el que resulta competente, las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Se entiende por dominio de seguridad el conjunto de infraestructuras de comunicaciones, equipamientos físicos y lógicos y personas que sobre ellos operan, interrelacionados de tal modo que resulte más eficiente gestionar la seguridad de la información manejada por los mismos de forma conjunta.

2. Se designarán los siguientes Responsables de Seguridad de la Información, según el dominio de seguridad en el que resulten competentes:

a) RSI cuyo ámbito de responsabilidad comprende la información y servicios afectados por los sistemas de información gestionados por el Ministerio de Sanidad, Servicios Sociales e Igualdad, así como los organismos públicos dependientes de éste y que no se incluyan dentro del ámbito de actuación del resto de RSI. Corresponderá al grupo técnico al que se refiere el apartado 3 del presente artículo.

b) RSI del IMSERSO. La designación corresponderá al titular de su Dirección General entre alguno de los efectivos que en ese momento presten servicios en el IMSERSO.

c) RSI de la ONT. La designación corresponderá al titular de su Dirección General entre alguno de los efectivos que en ese momento presten servicios en la ONT.

d) RSI de los Centros de Ceuta y Melilla (Direcciones Territoriales, Gerencias de Atención Especializada y Gerencias de Atención Primaria). La designación corresponderá al titular de la Dirección del INGESA entre alguno de los efectivos que en ese momento presten servicios en el INGESA.

3. El grupo técnico de seguridad de la información en el ámbito departamental estará presidido y coordinado por el titular de la Subdirección General de Tecnologías de la Información, y estará compuesto por los siguientes miembros:

a) El titular de la Subdirección General de Recursos Humanos.
b) El titular de la Subdirección General de Oficialía Mayor.
c) El titular de la Subdirección General de Normativa.
d) El titular de la Subdirección General de la Inspección General de Servicios.
e) Un representante por cada uno de los organismos públicos, designados por los titulares de aquellos.
f) Un funcionario dependiente de la Subdirección General de Tecnologías de la Información y designado por el titular de la misma, quien ejercerá las funciones de Secretario y coordinará al Equipo de Seguridad de la Información.

4. Serán funciones del RSI las siguientes, en su dominio:

a) Impulsar y revisar un Sistema de Gestión de Seguridad de la Información (en adelante SGSI), de acuerdo al estándar UNE-ISO/IEC 27001, para el dominio de seguridad que le corresponda.

cve: BOE-A-2014-2378

b) Coordinar la realización del Análisis de Riesgos anual sobre los sistemas de información bajo su responsabilidad.

c) Aprobar la normativa de seguridad derivada de tercer nivel (procedimientos generales).

d) Coordinar y controlar el cumplimiento de las medidas de seguridad definidas en los documentos de seguridad correspondientes a todos los ficheros o tratamientos de datos de carácter personal existentes.

e) Mantener el marco documental relativo al sistema de gestión de la seguridad de la información actualizado.

f) Determinar los controles de la norma UNE-ISO/IEC 27002 necesarios para mitigar el riesgo resultante del Análisis de Riesgos.

g) Elaborar el plan de proyectos anual y coordinar su ejecución.

h) Operar los recursos facilitados por el Comité.

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

j) Gestionar los incidentes de seguridad de la información que se produzcan, informando de los más relevantes al Comité.

k) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

l) Designar el auditor interno de la seguridad de la información.

m) Elaborar el Informe de Revisión por Dirección anual.

n) Definir, revisar y ajustar los indicadores de eficacia necesarios para controlar el estado del SGSI.

o) Coordinar a los responsables de la información y a los de los servicios.

p) Informar sobre el estado de las principales variables de seguridad en los sistemas de información del dominio de seguridad correspondiente al Comité de Seguridad de la Información de las Administraciones Públicas para la elaboración de un perfil general del estado de seguridad de las mismas.

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

Artículo 7. *Equipo de Seguridad de la Información.*

1. El Equipo de Seguridad de la Información se constituye como grupo de apoyo del RSI correspondiente para el cumplimiento de sus funciones.

2. A estos efectos, el Equipo de Seguridad de la Información realizará las auditorías periódicas de seguridad (prevención), el seguimiento y control del estado de seguridad del sistema (detección), la respuesta eficaz a los incidentes de seguridad desde su notificación hasta su resolución (respuesta) y el desarrollo de los planes de continuidad de los sistemas de información (recuperación).

3. El RSI correspondiente determinará la composición del Equipo de Seguridad de la Información entre los efectivos que en ese momento presten servicios en el Departamento u organismo público dependiente de que se trate.

Artículo 8. *El Responsable de la Información.*

1. El Responsable de la Información es el titular del órgano o unidad que gestione cada procedimiento administrativo.

En los casos en que un sistema trate datos de carácter personal, el Responsable de la Información será además el responsable del fichero. Sus funciones vendrán determinadas por la legislación aplicable sobre protección de datos de carácter personal.

2. El Responsable de la Información tiene encomendada la función de determinar los niveles de seguridad de la información dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero.

cve: BOE-A-2014-2378

3. Será además responsable frente a cualquier error o negligencia dentro del procedimiento administrativo que gestione y que lleve a un incidente de confidencialidad o de integridad.

Artículo 9. *El Responsable del Servicio.*

1. El Responsable del Servicio es el titular del órgano o unidad que gestione cada servicio.
2. El Responsable del Servicio tiene encomendada la función de determinar los niveles de seguridad del servicio dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero.

Artículo 10. *Resolución de conflictos.*

1. En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En su defecto, será el Comité quien resuelva.
2. En la resolución de estos conflictos, prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

Artículo 11. *Gestión de 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, de conformidad con lo dispuesto en el artículo 6 del Real Decreto 3/2010, de 8 de enero, y en la reevaluación periódica.
2. El RSI es el encargado de que el análisis se realice en tiempo y forma, así como de identificar carencias y debilidades y ponerlas en conocimiento de los Responsables de la Información y del Servicio.
3. La 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 proporcionadas a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el Responsable de Seguridad de la Información correspondiente al dominio de seguridad, recogiéndose en un Plan de Acción anual.
4. En particular, para realizar el análisis de riesgos se utilizarán las herramientas PILAR o μPILAR que facilitan el seguimiento de la aplicación de las medidas de seguridad seleccionadas y proporcionan un valor de riesgo residual estabilizado y comparable entre diferentes sistemas de información.

Artículo 12. *Desarrollo normativo.*

1. El cuerpo normativo sobre seguridad de la información se desarrollará en cinco niveles con diferente ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, pero de manera que cada elemento normativo se fundamente en las normas de nivel superior.

Todos estos niveles prestarán especial atención a las exigencias derivadas del Esquema Nacional de Seguridad, así como a la normativa aplicable en materia de protección de datos de carácter personal.

Los niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: PSI. Está constituido por la presente orden, que en el anexo establece las directrices generales para la gestión de la seguridad de la información, fundamentada en la norma UNE-ISO/IEC 27002. Es de obligado cumplimiento en todo el Ministerio de Sanidad, Servicios Sociales e Igualdad, organismos públicos y entidades colaboradoras con estos.

cve: BOE-A-2014-2378

b) Segundo nivel normativo: Normas de seguridad. Son de obligado cumplimiento en todo el Ministerio de Sanidad, Servicios Sociales e Igualdad, en los elementos que apliquen a cada dominio de seguridad. Son las siguientes:

1. Clasificación y tratamiento de la información.
2. Roles y responsabilidades de seguridad.
3. Seguridad física.
4. Gestión de operaciones.
5. Control de accesos.
6. Adquisición y desarrollo de sistemas.
7. Gestión de incidentes de seguridad.
8. Continuidad de negocio.
9. Adecuación a la legislación vigente.

c) Tercer nivel normativo: Procedimientos generales. Describen las acciones a realizar en un proceso relacionado con la seguridad, responsabilidad de varias unidades organizativas, dentro de un mismo dominio de seguridad. Son dependientes de las normas.

d) Cuarto nivel normativo: Procedimientos específicos. Describen las acciones a realizar en un proceso relacionado con la seguridad, responsabilidad de una unidad organizativa, dentro de un mismo dominio de seguridad. Dependen de normas o de procedimientos generales.

e) Quinto nivel normativo: Informes, registros, evidencias electrónicas y plantillas. Los informes son documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o de una evaluación. Los registros de actividad o alertas de seguridad son documentos de carácter técnico que recogen amenazas y vulnerabilidades a sistemas de información y son responsabilidad del equipo de seguridad. Las evidencias electrónicas se generan durante todo el ciclo de vida de los sistemas de información, pudiendo abarcar uno o más sistemas en función del aspecto tratado.

2. El Comité 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.

La siguiente tabla resume el marco normativo y la responsabilidad de su aprobación.

Nivel normativo	Documento	Aprueba
Primero.	Política de Seguridad.	Órgano superior competente.
Segundo.	Normas de Seguridad.	Comité de Seguridad de la Información.
Tercero.	Procedimientos generales.	Responsable de Seguridad de la Información.
Cuarto.	Procedimientos específicos.	Unidad implicada.
Quinto.	Informes, registros, evidencias y plantillas.	Equipo de Seguridad de la Información.

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

1. Serán responsables de los ficheros que contengan datos de carácter personal las personas definidas en el artículo 8.1.

2. Los ficheros que contengan datos de carácter personal estarán referenciados en el correspondiente documento de seguridad previsto en el artículo 88 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre.

3. Las medidas de seguridad requeridas por el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, estarán incluidas en los diferentes niveles de desarrollo normativo previstos en el artículo 12.

cve: BOE-A-2014-2378

Artículo 14. *Formación.*

En el Ministerio de Sanidad, Servicios Sociales e Igualdad, se desarrollarán actividades específicas orientadas a la formación de su personal en materia de seguridad de la información, así como a la difusión de la PSI y su desarrollo normativo.

A estos efectos, deberán incluirse actividades formativas en esta materia dentro de los Planes de Formación del Ministerio.

Disposición adicional primera. *Actualización permanente y revisiones periódicas de la PSI.*

1. Esta orden deberá mantenerse actualizada para adecuarla al progreso de los servicios de Administración Electrónica, a la evolución tecnológica y al desarrollo de la sociedad de la información, así como a los estándares internacionales de seguridad.

2. Las propuestas de las sucesivas revisiones de la PSI las hará el Comité.

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

La aplicación de esta orden no conllevará incremento de gasto público. Las medidas incluidas en la misma no supondrán, en ningún caso, incremento de dotaciones ni de retribuciones ni de otros gastos de personal.

Disposición final primera. *Deber de colaboración de órganos y unidades del Departamento.*

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

Disposición final segunda. *Publicidad de la PSI.*

Esta orden se publicará, además de en el «Boletín Oficial del Estado», en cada una de las sedes electrónicas del Ministerio de Sanidad, Servicios Sociales e Igualdad.

Disposición final tercera. *Entrada en vigor.*

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

Madrid, 26 de febrero de 2014.–La Ministra de Sanidad, Servicios Sociales e Igualdad, Ana Mato Adrover.

ANEXO

Directrices generales para el establecimiento de un marco de control de la seguridad de la información y para la determinación de los objetivos de control de la seguridad necesarios, basados en el estándar internacional ISO/IEC 27002:2005

Gestión de los activos:

• Se deberá conseguir y mantener un nivel apropiado de protección sobre los activos del Ministerio, prestando especial atención a aquellos que contengan datos de carácter personal.

• Todos los activos de información tendrán un propietario, asignándole la responsabilidad del mantenimiento de los controles apropiados. La implantación de los controles específicos puede ser delegada por el propietario según considere pero la responsabilidad de la adecuada protección de los activos permanece en él.

• Toda la información deberá ser inventariada y clasificada en función de unos niveles establecidos en base a su sensibilidad y criticidad.

cve: BOE-A-2014-2378

• Se definirán normas de uso aceptable de los activos (correo electrónico, Internet, dispositivos móviles, documentación en papel, etc.).

Seguridad relacionada con los recursos humanos:

• Se velará porque empleados, contratistas y terceras partes entiendan sus responsabilidades y estas sean adecuadas a sus roles asignados, con objeto de reducir el riesgo de hurto, fraude o mal uso de las instalaciones.

• Todo el personal con acceso a la información deberá ser consciente de las amenazas a la seguridad de la información, siendo conocedor de sus responsabilidades y obligaciones (con especial atención a las exigencias establecidas en la normativa en materia de protección de datos de carácter personal) y estando preparado para aplicar la política y normas de seguridad en el curso de su trabajo habitual.

• Se deberá asegurar que todo proceso de salida de personal de la Organización (o cambio de puesto) se haga de una forma gestionada, realizándose las comunicaciones oportunas de forma temprana y controlando la devolución de activos y la retirada de los derechos de acceso otorgados.

Seguridad física y del entorno:

• La información y los sistemas que la soportan, se ubicarán en áreas seguras adecuadamente protegidas de amenazas físicas o ambientales, sean estas intencionadas o accidentales. La protección suministrada deberá ser siempre proporcional al riesgo y función de la criticidad de la información, con especial atención a la seguridad de los datos de carácter personal. Será necesario establecer las suficientes garantías físicas de seguridad, a fin de reducir los riesgos de daños o pérdidas de datos.

• Las instalaciones de procesamiento de la información y la información deben ser protegidas contra la divulgación, modificación o robo de la información, así como de accesos físicos no autorizados, debiéndose implementar controles para minimizar pérdidas o daños.

• Existirá un plan de emergencia y evacuación del edificio para el caso de amenazas físicas o ambientales, cuyo objetivo primordial sea la protección de las personas.

Gestión de comunicaciones y operaciones:

• Se debe asegurar el funcionamiento correcto y seguro de los recursos de tratamiento de la información, estableciendo las responsabilidades y los procedimientos para la gestión y operación de todos los recursos de información, incluyendo la documentación de los mismos.

• Se implantará una segregación de tareas donde sea apropiado, para reducir el riesgo de negligencia o uso incorrecto e intencionado

• Se implementará y velará por el mantenimiento de un nivel apropiado de seguridad de la información y de niveles de servicio en línea con los acuerdos firmados con terceras partes.

• Se comprobará el cumplimiento y conformidad con los acuerdos, gestionando los cambios necesarios para asegurar que los servicios entregados son conformes con todos los requisitos acordados con la tercera parte.

• Con objeto de minimizar el riesgo de fallos en los sistemas, se realizarán estudios para futuros requerimientos de capacidad, a fin de reducir los riesgos de sobrecarga de los sistemas y garantizar la disponibilidad de capacidad. Se deberán establecer, documentar y probar previamente a su aceptación y uso los requisitos operacionales de los sistemas nuevos.

• Existirán mecanismos adecuados para el control de software malicioso, prestando especial atención a la concienciación de los usuarios acerca de los peligros del software no autorizado y malicioso.

• Se crearán los procedimientos necesarios para garantizar la integridad y disponibilidad de la información y los recursos de tratamiento de la información. Se

cve: BOE-A-2014-2378

establecerán procedimientos rutinarios de copias de seguridad de datos y de verificación de la posible restauración mediante las copias.

• La gestión de seguridad de las redes que atraviesan el perímetro del Ministerio requerirá la implantación de controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas.

• Los medios de almacenamiento de información serán controlados y protegidos físicamente estableciendo procedimientos operativos apropiados para prevenir la revelación, modificación, eliminación o destrucción no autorizada.

• Se controlará el intercambio de información y software entre organizaciones, siendo consecuentes con la legislación aplicable. Asimismo, existirán procedimientos que garanticen la protección de la información y los medios en tránsito.

• La integridad de la información almacenada en sistemas accesibles públicamente estará protegida para prevenir su integridad y disponibilidad.

Control de acceso:

• Los procedimientos para el control de acceso a los sistemas de información deberán cubrir todas las etapas del ciclo de vida de los accesos de un usuario, prestando una concreta atención al acceso a sistemas de información que contengan datos de carácter personal. El acceso no autorizado a los sistemas y servicios de información deberá ser evitado, implementando controles apropiados para la gestión de los derechos de usuario basándose en una política de control de acceso.

• Se concienciará a los usuarios acerca de sus responsabilidades en el mantenimiento de las medidas de control de acceso, particularmente en el uso de credenciales y en la seguridad de su equipamiento habitual.

• El acceso a la información y los recursos de tratamiento serán otorgados sobre la base de los requisitos mínimos indispensables de accesos de los usuarios para el desempeño de sus funciones.

• Los accesos a la información deberán ser monitorizados, a fin de comprobar la eficacia de los controles adoptados y detectar las desviaciones respecto de la política de control de accesos.

• Deberá garantizarse la seguridad de la información en el uso de dispositivos móviles e instalaciones de trabajo remotas. La protección requerida será proporcional al riesgo que implique la modalidad de trabajo.

Adquisición, desarrollo y mantenimiento de sistemas de información:

• Se deberá garantizar que la seguridad sea una parte integral de los sistemas de información. Para ello, los requisitos de seguridad serán identificados, justificados, acordados y documentados durante la fase de requisitos de los proyectos, considerándose así desde las primeras etapas del ciclo de vida de los sistemas.

• Se deberá garantizar el procesamiento correcto de las aplicaciones, evitando errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones, introduciendo controles de validación de datos, pistas de auditoría y los registros de actividad necesarios.

• Cuando una información sea crítica, se protegerá mediante el uso de medios criptográficos, amparándose en una política interna de uso de este tipo de controles que regule su uso.

• Se controlarán estrictamente los entornos de los proyectos y el soporte a los mismos. Los propietarios de los sistemas de aplicación también serán responsables de la seguridad de los mismos, garantizando que todos los cambios propuestos sean revisados, a fin de comprobar que los mismos no comprometen la seguridad del sistema.

• Se velará por la seguridad de los ficheros de sistema y código fuente de las aplicaciones, evitando el acceso y modificación no autorizado.

• Se implementarán mecanismos para reducir el riesgo resultante de la probabilidad de explotación de vulnerabilidades técnicas, manteniendo la seguridad de las aplicaciones y programas.

cve: BOE-A-2014-2378

• La seguridad de los sistemas de información garantizará en todo caso el pleno respeto a las garantías determinadas por la normativa en materia de datos de carácter personal.

Gestión de incidencias de seguridad de la información:

• Se dispondrán los medios para garantizar que los eventos que afecten a la seguridad de la información y las debilidades asociadas a los sistemas (especialmente en aquellos supuestos que afecten a datos de carácter personal) sean comunicados de forma tal que las acciones correctivas correspondientes sean aplicadas de manera oportuna y adecuada.

• Deberán existir procedimientos formales de comunicación y escalado de incidentes. Todos los trabajadores, contratistas y terceros deberán conocer los procedimientos establecidos y estarán obligados a comunicarlos al contacto designado.

• Deberán existir responsabilidades y procedimientos para tratar dichos incidentes, aplicándose un proceso de mejora continua a la reacción, supervisión, evaluación y la gestión general de los mismos. Cuando sean necesarias pruebas, éstas deberán recopilarse para garantizar el cumplimiento de los requisitos legales.

Gestión de la continuidad del negocio:

• Deberá implementarse un proceso de gestión de la continuidad del negocio para asegurar la protección de los servicios críticos del Ministerio, con especial atención a aquellos que afecten a datos de carácter personal, así como su recuperación en el tiempo requerido tras un desastre o fallo importante de los sistemas de información.

• La continuidad de las actividades críticas del Ministerio estará respaldada por la existencia de un grupo de gestión de crisis, con la suficiente capacidad de decisión, y unos adecuados controles preventivos y de recuperación a fin de reducir los fallos de los sistemas a un nivel aceptable.

• La gestión de la continuidad del negocio deberá incluir, además del proceso general de evaluación de riesgos, controles para identificar y reducir los riesgos, limitar las consecuencias de incidentes dañinos y garantizar que la información necesaria para los servicios esté disponible.

• Los planes de continuidad del negocio deberán probarse y actualizarse periódicamente para garantizar que están al día y que son efectivos.

Conformidad:

• Se deberán evitar quebrantamientos de las leyes o incumplimientos de cualquier obligación legal, reglamentaria, contractual o de cualquier requisito de seguridad en relación con el diseño, operación, uso y administración de la información y los sistemas de tratamiento. Se observará especialmente la normativa aplicable en materia de protección de datos de carácter personal.

• Con el fin de conseguir la conformidad de los sistemas con las políticas y normas de seguridad del Ministerio, se realizarán revisiones regulares y auditorías de los sistemas de información, basándose en las políticas de seguridad apropiadas, para ver el grado de implantación y cumplimiento, con especial respeto a la normativa aplicable en materia de protección de datos de carácter personal.

cve: BOE-A-2014-2378