III. OTRAS DISPOSICIONES

MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO

5575 *Orden ITC/657/2011, de 11 de marzo, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Industria, Turismo y Comercio.*

El desarrollo de la Administración Electrónica implica el tratamiento de ingentes 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 la Administración Electrónica se entiende por seguridad 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 (ENS) en el ámbito de la Administración Electrónica, persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiaran 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.

El Real Decreto 3/2010, de 8 de enero, enuncia en sus artículos 5 a 10 los principios básicos en materia de seguridad de la información (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica y función diferenciada) y establece el marco regulatorio de la Política de Seguridad de la Información (PSI), que se plasma en un documento, accesible y comprensible para todos los miembros, que define lo que significa seguridad de la información en una organización determinada y que rige la forma en que una organización gestiona y protege la información y los servicios que considera críticos, disponiendo que:

1. Todos los órganos superiores, esto es, Ministerios y Secretaría de Estado en la Administración General del Estado (AGE), deberán disponer formalmente de su PSI, que será aprobada por el titular del órgano superior correspondiente (artículo 11).
2. La PSI debe comprometer a todos los miembros de la organización, por los que debe ser conocida, e identificar unos claros responsables de velar por su cumplimiento (artículo 12).
3. El contenido mínimo de la PSI debe precisar de forma clara los objetivos o misión de la organización, el marco legal y regulatorio en que desarrolla sus actividades, los roles o funciones de seguridad, definiendo para cada uno sus deberes y responsabilidades, así como el procedimiento para su designación y renovación, la estructura del comité para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, sus miembros y su relación con otros elementos de la organización, y las directrices para la estructuración de de la documentación de seguridad del sistema, su gestión y acceso [anexo II.3 Política de Seguridad (org 1)].
4. Además, la PSI debe ser coherente con lo establecido en el Documento de Seguridad que exige el artículo 88 del 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, en lo que corresponda, prevaleciendo lo relativo a la protección de datos de carácter personal en caso de discrepancias.
5. Para la elaboración de la PSI deben utilizarse las guías CCN-STIC 001, 201, 402, 801 y 805 elaboradas por el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI), que establecen las pautas de carácter general relativas a la

cve: BOE-A-2011-5575

organización de seguridad y sus responsables, así como sobre la estructura y contenido mínimo de la PSI.

El artículo 11 del Real Decreto 3/2010, de 8 de enero, establece que todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente.

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 Industria, Turismo y Comercio, así como el establecimiento del marco organizativo y tecnológico de la misma.

2. La PSI que se aprueba por esta orden se aplicará con carácter imperativo por todos los órganos y unidades centrales y territoriales del Ministerio de Industria, Turismo y Comercio, así como por los organismos autónomos que dependan de los mismos (Oficina Española de Patentes y Marcas, Instituto para la Reestructuración de la Minería del Carbón y Desarrollo Alternativo de las Comarcas Mineras, Centro Español de Metrología e Instituto de Turismo de España), siendo de aplicación a todos sus sistemas de información y debiendo ser observada 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.

Artículo 2. *Misión del Departamento.*

Corresponde al Ministerio de Industria, Turismo y Comercio la propuesta y ejecución de la política del Gobierno en materia de desarrollo industrial, política comercial, política energética, política de la pequeña y mediana empresa (PYME), política de turismo y política de telecomunicaciones y de la sociedad de la información.

Artículo 3. *Marco normativo.*

1. El marco normativo en que se desarrollan las actividades del Ministerio de Industria, Turismo y Comercio, y, en particular, la prestación de sus servicios electrónicos a los ciudadanos, está integrado por las siguientes normas:

a) La legislación sectorial reguladora de la actuación de los órganos superiores y directivos del Ministerio de Industria, Turismo y Comercio y de los organismos autónomos dependientes, así como el Real Decreto 1226/2010, de 1 de octubre, por el que se desarrolla la estructura orgánica básica de dicho Departamento ministerial.

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) 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.

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 el documento nacional de identidad y sus certificados de firma electrónica.

cve: BOE-A-2011-5575

j) Orden ITC/164/2010, de 28 de enero, por la que se crea la sede electrónica en el Ministerio de Industria, Turismo y Comercio, así como las otras normas que hayan creado o puedan crear otras sedes electrónicas dentro del ámbito de aplicación de la PSI.

k) Orden ITC/1515/2010, de 8 de junio, por la que se crea el registro electrónico en el Ministerio de Industria, Turismo y Comercio, así como las otras normas que hayan creado o puedan crear otros registros electrónicos dentro del ámbito de aplicación de la PSI.

2. También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Departamento derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación 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 Industria, Turismo y Comercio está compuesta por los siguientes agentes:

a) El Comité para la Gestión y Coordinación de la Seguridad de la Información.
b) El Responsable de Seguridad.
c) El Responsable de la Información.
d) El Responsable del Servicio.

Artículo 5. *El Comité para la Gestión y Coordinación de la Seguridad de la Información.*

1. Se crea el Comité para la Gestión y Coordinación de la Seguridad de la Información (en adelante, el Comité), que 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.
b) Aprobar la normativa de seguridad derivada de segundo nivel que sea de obligado cumplimiento (procedimientos STIC, normas STIC e instrucciones técnicas STIC).
c) Aprobar el procedimiento de control de accesos a la red y a las bases de datos de la Administración Electrónica del Ministerio de Industria, Turismo y Comercio, así como los demás procedimientos de actuación en lo relativo al uso de los sistemas de información.
d) Determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
e) Coordinar la comunicación con el Centro Criptológico Nacional en la utilización de servicios de respuesta a incidentes de seguridad.
f) Informar sobre el estado de las principales variables de seguridad en los sistemas de información 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.
g) Compartir experiencias de éxito en materia de seguridad entre sus miembros para velar por el cumplimiento de la PSI y su normativa de desarrollo.

2. El Comité estará compuesto por los siguientes miembros:

a) Presidente: La Secretaria General Técnica.
b) Vocales: Con categoría mínima de Subdirector General o asimilado, pudiendo delegar en un suplente por cada uno de los siguientes órganos u organismos autónomos del Departamento:

1. Secretaría de Estado de Comercio Exterior.
2. Secretaría de Estado de Energía.
3. Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.
4. Secretaría General de Industria.
5. Secretaría General de Turismo y Comercio Interior.
6. Oficina Española de Patentes y Marcas.

cve: BOE-A-2011-5575

7. Instituto para la Reestructuración de la Minería del Carbón y Desarrollo Alternativo de las Comarcas Mineras.
8. Centro Español de Metrología
9. Instituto de Turismo de España.

c) Secretario: con voz y voto, el Subdirector General de Tecnologías de la Información y de las Comunicaciones, que ejecutará las decisiones del Comité, convocará sus reuniones y preparará los temas a tratar.

3. El Comité podrá recabar del personal técnico propio o externo la información pertinente para la toma de sus decisiones.

Artículo 6. *El Responsable de Seguridad.*

1. Las funciones del Responsable de Seguridad se ejercerán por el grupo técnico de seguridad de la información, presidido y coordinado por el Subdirector General de Tecnologías de la Información y de las Comunicaciones y estará compuesto por los siguientes miembros:

a) Subdirector General de Coordinación Territorial y de Medios de la Secretaría de Estado de Comercio Exterior.
b) El Subdirector General de Fomento Empresarial de la Secretaría General de Industria.
c) El Director de la División de Tecnologías de la Información de la Oficina Española de Patentes y Marcas.
d) El Secretario General del Instituto para la Reestructuración de la Minería del Carbón y Desarrollo Alternativo de las Comarcas Mineras.
e) El Director del Centro Español de Metrología
f) El Secretario General del Instituto de Turismo de España.
Cada uno de los miembros podrá delegar en un suplente.

2. Serán funciones del Responsable de Seguridad las siguientes:

a) Mantener la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
b) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
c) Realizar el seguimiento y control del estado de seguridad del sistema de información.
d) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
e) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
f) Elaborar informes periódicos de seguridad para el Comité que incluyan los incidentes más relevantes de cada período.

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

Artículo 7. *Equipo de seguridad.*

1. Como grupo de apoyo del Responsable de Seguridad para el cumplimiento de sus funciones, éste contará con un equipo de seguridad que aglutinará las tareas de prevención de incidentes de seguridad, detección de anomalías, mecanismos de respuesta eficaz ante los mismos y actividades de recuperación mediante el desarrollo de planes de

cve: BOE-A-2011-5575

continuidad de los sistemas de información para garantizar la disponibilidad de los servicios críticos.

2. A estos efectos, el equipo de seguridad 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. La composición del equipo de seguridad se determinará por el Responsable de Seguridad, que también podrá designar equipos de seguridad delegados para el apoyo en estas tareas de los responsables de seguridad delegados.

Artículo 8. *El Responsable de la Información.*

1. El Responsable de la Información es la persona que determina los niveles de seguridad de la información dentro del marco establecido en el anexo I 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, previa propuesta del responsable de seguridad.

2. Esta responsabilidad recaerá en el 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.

Artículo 9. *El Responsable del Servicio.*

1. El Responsable del Servicio es la persona que determina los niveles de seguridad de los servicios dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, previa propuesta del Responsable de Seguridad.

2. Esta responsabilidad recaerá en el titular del órgano responsable del desarrollo, mantenimiento y explotación del sistema de información que soporte los servicios correspondientes.

3. Las funciones del Responsable del Servicio serán las siguientes:

a) Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, así como aprobar los cambios que afecten a la seguridad del modo de operación del sistema.

b) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

c) Realizar el preceptivo proceso de análisis y gestión de riesgos del sistema.

d) Determinar 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.

e) Establecer planes de contingencia y emergencia.

f) Suspender, previo acuerdo de los Responsables de Seguridad y de Información, el manejo de una determinada información o la prestación de un servicio electrónico si es informado de deficiencias graves de seguridad.

Artículo 10. *Resolución de conflictos.*

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad.

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 (artículo 6 Real Decreto 3/2010, de 8 de enero) y reevaluación periódica (artículo 9 Real Decreto 3/2010, de 8 de enero), siendo el Responsable del Servicio el encargado de que

cve: BOE-A-2011-5575

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

2. El Responsable de Seguridad 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. 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 proporcionadas 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.

6. En particular, para realizar el análisis de riesgos se podrán utilizar 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 cuatro 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:

1. Primer nivel normativo. PSI.–Está constituido por la presente orden y es de obligado cumplimiento.

2. Segundo nivel normativo. Normativa y recomendaciones de seguridad.–Está constituido por la normativa y recomendaciones de seguridad que se definan en cada ámbito organizativo de aplicación específico (órganos superiores y directivos, organismos públicos dependientes, etc.).

La normativa, que comprende los procedimientos STIC, las normas STIC y las instrucciones técnicas STIC, es de obligado cumplimiento y se formalizará mediante instrucciones o resoluciones de los titulares de los órganos correspondientes, previa aprobación del Comité, mientras que las recomendaciones consistirán en buenas prácticas y consejos no vinculantes para mejorar las condiciones de seguridad.

3. Tercer nivel normativo. Procedimientos técnicos (Guías STIC).–Está constituido por el conjunto de procedimientos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. Son recomendaciones o informaciones relativas a temas concretos de seguridad basadas en Instrucciones previas, que establecen las configuraciones mínimas de seguridad de los diferentes elementos de un sistema de información, recomendaciones de uso o de otro tipo.

La responsabilidad de aprobación de estos procedimientos técnicos dependerá de su ámbito de aplicación, que podrá ser en un ámbito específico o en un sistema de información determinado. Se consideran incluidas en este nivel normativo las guías CCN-STIC de las series 400-500- 600.

4. Cuarto nivel normativo. Informes, registros y evidencias electrónicas.–Está constituido por los informes técnicos, que son documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o de una evaluación; registros de actividad o alertas de seguridad, que son documentos de carácter técnico que recogen amenazas y vulnerabilidades a sistemas de información y son responsabilidad del equipo de seguridad;

cve: BOE-A-2011-5575

y evidencias electrónicas, que se generan durante todas las fases del ciclo de vida de los sistemas de información y en sus distintos procesos, 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.

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

1. Respecto a la protección de datos de carácter personal, el Responsable de la Información asumirá las funciones de responsable del fichero y el Responsable del Servicio las del responsable del tratamiento, siendo asumidas por el Responsable de Seguridad las funciones enumeradas en el artículo 6.

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

Artículo 14. *Formación y concienciación.*

1. Con la colaboración, en su caso, del Centro Criptológico Nacional, 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. A estos efectos, deberán incluirse actividades formativas en esta materia dentro de los Planes de Formación del Ministerio de Industria, Turismo y Comercio.

Artículo 15. *Actualización permanente y revisiones periódicas de la PSI.*

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

2. Las propuestas de las sucesivas revisiones de la PSI se elaborarán por el Comité y si su contenido es técnico podrán ser aprobadas por la Subsecretaria de Industria, Turismo y Comercio, produciendo efectos a partir de su publicación en la sede electrónica del Departamento.

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

La aplicación de esta orden no conllevará incremento de gasto público, atendiéndose el funcionamiento del Comité con los recursos humanos y materiales de que dispone el Ministerio de Industria, Turismo y Comercio.

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

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

Disposición final segunda. *Publicidad de la PSI.*

La presente orden se publicará, además de en el «Boletín Oficial del Estado», en la sede electrónica del Ministerio de Industria, Turismo y Comercio,

Disposición final tercera. *Aplicabilidad.*

La PSI que se aprueba en esta orden será aplicable a partir del día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 11 de marzo de 2011.–El Ministro de Industria, Turismo y Comercio, Miguel Sebastián Gascón.

cve: BOE-A-2011-5575