III. OTRAS DISPOSICIONES

MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

10732 *Orden IET/1934/2014, de 14 de octubre, por la que se establece la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Industria, Energía y Turismo.*

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 (TIC), que está sometida a diferentes tipos de amenazas y vulnerabilidades.

La Estrategia de Seguridad Nacional (ESN) aprobada en Consejo de Ministros el 31 de Mayo de 2013 busca incrementar la capacidad de prevención, detección, investigación y respuesta ante las nuevas ciberamenazas y garantizar la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones públicas, a la vez que se mejora la seguridad y resiliencia de las tecnologías TIC en el sector privado a través del uso de las capacidades de los poderes públicos, y se fomenta la capacitación de profesionales en ciberseguridad y la concienciación ciudadana.

El reconocimiento de que el desarrollo de las tecnologías TIC ha generado un nuevo espacio de relación para nuestra sociedad, el ciberespacio, se ha plasmado en la Estrategia de Ciberseguridad Nacional (ECSN), aprobada por el Consejo de Seguridad Nacional el 5 de diciembre de 2013, mediante la cual se pretende fijar las directrices generales de uso del ciberespacio, impulsando una visión integradora cuya aplicación ayude a garantizar la seguridad y progreso de nuestra nación, a través de la adecuada coordinación y cooperación de todas las Administraciones públicas entre ellas, con el sector privado y con los ciudadanos.

Por otra parte, para contribuir al rápido desarrollo de la sociedad de la información, es indispensable trabajar por el fomento de un clima de confianza que garantice la seguridad de la información, las infraestructuras de red, la autenticación, la privacidad y la protección de los consumidores y los usuarios TIC que, a nivel de la Administración pública, se ha plasmado en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS).

El Real Decreto 3/2010, de 8 de enero, enuncia 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, la cual se plasmará en un documento, accesible y comprensible para toda la organización, 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, 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 para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

La aportación del Ministerio de Industria, Energía y Turismo al conjunto global de medidas destinadas a proteger la información, entre las que se encuentra la ESN y la ECSN, junto con el cumplimiento de lo dispuesto en el Real Decreto 3/2010, de 8 de enero, demanda la aprobación de una Política de Seguridad de la Información, que recoja la estructura normativa a desarrollar e implantar mediante medidas técnicas concretas.

cve: BOE-A-2014-10732

Durante el proceso de tramitación del texto de referencia de la mencionada Política de Seguridad de la Información, se ha recabado de forma favorable el informe de la Secretaría General Técnica del Ministerio de Industria, Energía y Turismo y el informe favorable del Ministerio de la Presidencia, a través del Centro Criptológico Nacional (CCN). Así mismo, el texto de referencia se ha presentado a trámite de audiencia ante la Comisión Permanente de la Comisión Superior de Administración Electrónica (CPCSAE), que emitió informe favorable con fecha 25 de junio de 2014.

En su virtud, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas, 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, Energía y Turismo, 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, Energía y Turismo, 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.

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 se esté afectada por la Ley 9/1968, de 5 de abril, sobre Secretos Oficiales.

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.

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. El Ministerio aplicará las medidas de seguridad sobre la información correspondientes, tanto en soporte electrónico como en papel, dependiendo de lo establecido en su normativa reguladora, pudiendo verse afectada una información concreta por más de una norma.

cve: BOE-A-2014-10732

Artículo 2. *Misión del Departamento.*

El Real Decreto 344/2012, de 10 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Industria, Energía y Turismo dispone que corresponde al Ministerio de Industria, Energía y Turismo la propuesta y ejecución de la política del Gobierno en materia de energía, de telecomunicaciones y de la sociedad de la información, de turismo y de desarrollo industrial y de la pequeña y mediana empresa.

Artículo 3. *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, Energía y Turismo está compuesta por los siguientes agentes:

a) El Comité Director de la Seguridad de la Información.
b) El Responsable de Seguridad.
c) El Responsable de la Información.
d) El Responsable del Servicio.

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

1. Se crea el Comité Director de la Seguridad de la Información (en adelante, el Comité), que gestionará y 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, Energía y Turismo, 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) Informar sobre el estado de las principales variables de seguridad en los sistemas de información al Comité Sectorial de Administración Electrónica (CSAE) para la elaboración de un perfil general del estado de seguridad de las mismas.
f) 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: El Subsecretario de Industria, Energía y Turismo.
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 General Técnica.
2. Secretaría de Estado de Energía.
3. Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.
4. Secretaría de Estado de Turismo.
5. Secretaría General de Industria y de la Pequeña y Mediana Empresa.
6. Oficina Española de Patentes y Marcas.
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.

cve: BOE-A-2014-10732

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.

d) Con carácter facultativo, el Presidente del Consejo de Administración del Instituto Nacional de Tecnologías de la Comunicación (INTECO) podrá formar parte del Comité como vocal, con voz, o bien delegar en un suplente con categoría mínima de Subdirector General o asimilado.

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

Artículo 5. *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, cada uno de los cuales podrá delegar en un suplente en caso necesario:

a) El Subdirector General de Apoyo a la Pequeña y Mediana Empresa.

b) El Director de la División de Tecnologías de la Información de la Oficina Española de Patentes y Marcas.

c) El Secretario General del Instituto para la Reestructuración de la Minería del Carbón y Desarrollo Alternativo de las Comarcas Mineras.

d) El Director del Centro Español de Metrología.

e) El Subdirector General de Gestión Económico-Administrativa y Tecnologías de la Información del Instituto de Turismo de España.

Los acuerdos y decisiones adoptados por los miembros que conforman el grupo técnico de seguridad de la información se harán por mayoría de sus miembros y su presidente contará con un voto de calidad en caso de empate.

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.

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

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.

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.

cve: BOE-A-2014-10732

Artículo 6. *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 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 7. *El Responsable de la Información.*

1. 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, y serán las siguientes:

a) 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, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, previa propuesta del Responsable de Seguridad.

b) Determinar las excepciones al punto anterior que sean de aplicación a la información de gestión interna. En este sentido, el Subsecretario es el responsable de establecer las medidas de protección y destrucción de la información de gestión interna y, singularmente, los órganos superiores podrán definir medidas de seguridad adicionales sobre cierta información que consideren sensible en el ámbito de sus Unidades y de acuerdo con el Responsable de Seguridad.

c) En el ámbito de la información que contenga datos de carácter personal velará por la aplicación de los niveles de protección que establezca el responsable del fichero, así como las medidas de seguridad aplicables a los ficheros que contengan datos de carácter personal, según lo dispuesto en el 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.

d) En el ámbito de la información susceptible de formar parte del patrimonio documental, velará por el cumplimiento de lo que establezca la Comisión Calificadora de Documentos Administrativos del Departamento.

e) En el ámbito de la información clasificada a la que sea de aplicación la Ley 9/1968, de 5 de abril, de Secretos Oficiales, el Responsable de la velará por el cumplimiento de lo que establezca la Autoridad Nacional de Seguridad.

Artículo 8. *El Responsable del Servicio.*

Las funciones del Responsable del Servicio recaerán en los titulares de los órganos responsables del desarrollo, mantenimiento y explotación del sistema de información que soporte los servicios correspondientes y 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.

cve: BOE-A-2014-10732

c) Realizar el preceptivo proceso de análisis y gestión de riesgos del sistema.
d) Establecer planes de contingencia y emergencia.
e) 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 9. *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 10. *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 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 11. *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:

a) Primer nivel normativo. PSI. Está constituido por la presente orden y es de obligado cumplimiento.
b) 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

cve: BOE-A-2014-10732

aprobación del Comité, mientras que las recomendaciones consistirán en buenas prácticas y consejos no vinculantes para mejorar las condiciones de seguridad.

c) 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 y 600.

d) 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; 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 12. *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 5.

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

Artículo 13. *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. A estos efectos, deberán incluirse actividades formativas en esta materia dentro de los planes de formación del Ministerio de Industria, Energía y Turismo.

Artículo 14. *Actualización permanente y revisiones periódicas de la PSI.*

La PSI 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.

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, Energía y Turismo.

cve: BOE-A-2014-10732

Disposición derogatoria. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo establecido en la presente orden y, en particular, la 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.

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 Departamento.

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, 14 de octubre de 2014.–El Ministro de Industria, Energía y Turismo, José Manuel Soria López.

cve: BOE-A-2014-10732