

III. OTRAS DISPOSICIONES

MINISTERIO DE FOMENTO

11118 Orden FOM/1987/2014, de 20 de octubre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Fomento.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos señala en su exposición de motivos, que «el principal reto que tiene la implantación de las Tecnologías de la Información y las Comunicaciones en la sociedad en general, y en la Administración en particular, es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización».

El artículo 3 de dicha Ley dispone que son fines de la misma, entre otros, «crear las condiciones de confianza en el uso de los medios electrónicos estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial, los relacionados con la intimidad y la protección de datos de carácter personal por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos».

El Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, regulado por el Real Decreto 3/2010, de 8 de enero, persigue fundamentar la confianza en que los sistemas de información que soporten la prestación de los servicios de administración electrónica y que manejen la información demandada por dichos servicios, lo harán con arreglo a sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Para lograr dicho propósito, resulta imprescindible acometer en primer lugar la organización global de la seguridad de la información. En la cúspide de dicha organización se sitúa la Política de Seguridad de la Información como documento destinado a recoger las directrices que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos.

El contenido de la política de seguridad de la información, recogerá los aspectos detallados en la sección 3.1 del Anexo II del Esquema Nacional de Seguridad, y además, será 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 Real Decreto 1720/2007, de 21 de diciembre, prevaleciendo lo relativo a la protección de datos de carácter personal en caso de discrepancias.

La presente Política de Seguridad de la Información afectará a los sistemas de información del Ministerio de Fomento, incluyendo los organismos autónomos y agencias estatales dependientes del Departamento, así como a las entidades colaboradoras con éstos sin excepciones.

En virtud de lo anterior, y en cumplimiento del artículo 11 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, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas, dispongo:

Artículo 1. Objeto y ámbito de aplicación.

1. Esta orden tiene por objeto aprobar la Política de Seguridad de la Información (en adelante PSI) en el ámbito de la Administración Electrónica del Ministerio de Fomento y establecer el marco organizativo y tecnológico de la misma.

2. La PSI se aplicará por todos los órganos superiores y directivos del Departamento y por los organismos públicos y agencias estatales, a todos los sistemas de información que gestionen en el ejercicio de sus competencias, debiendo ser cumplida por su personal y por cualquiera que tenga acceso a sus sistemas de información.

Artículo 2. *Misión.*

Al Ministerio de Fomento le corresponde la propuesta y ejecución de la política del Gobierno en los ámbitos de las infraestructuras de transporte terrestre, aéreo y marítimo, de competencia estatal; de control, ordenación y regulación administrativa de los servicios de transporte correspondientes; de acceso a la vivienda, edificación, urbanismo, suelo y arquitectura, en el ámbito de las competencias de la Administración General del Estado; de ordenación normativa de los servicios postales; de impulso y dirección de los servicios estatales relativos a astronomía, geodesia, geofísica y cartografía; y de planificación y programación de las inversiones relativas a las infraestructuras, materias y servicios mencionados.

Artículo 3. *Marco normativo.*

1. El marco normativo de las actividades de la PSI está integrado por todas las normas vigentes que afecten a la seguridad de la información en el ámbito de la Administración Electrónica del Ministerio de Fomento.

2. Las acciones que el Ministerio de Fomento emprenda en materia de seguridad de la información serán acordes con las mejores prácticas de seguridad, recogidas en las guías del CCN-STIC del Centro Criptológico Nacional y otras normas internacionalmente reconocidas.

Artículo 4. *Estructura organizativa.*

La estructura organizativa de la PSI en el Ministerio de Fomento estará compuesta por los siguientes agentes:

- a) El Comité de Seguridad de la Información,
- b) El responsable de Seguridad,
- c) El responsable de la Información,
- d) El responsable del Servicio.

Artículo 5. *El Comité de Seguridad de la Información del Ministerio de Fomento.*

1. Se crea el Comité de Seguridad de la Información (en adelante el Comité) como grupo de trabajo en el seno de la Comisión Ministerial de Administración Electrónica del Ministerio de Fomento.

2. El Comité estará compuesto por los siguientes miembros:

- a) Presidente: La persona titular de la Inspección General de Fomento.
- b) Vocales: Un representante, con rango mínimo de Subdirector General o asimilado, de cada uno de los órganos directivos del Ministerio de Fomento, así como de los organismos autónomos y agencias estatales dependientes del Departamento.
- c) Secretario: La persona titular de la Subdirección General de Tecnologías de la Información y Administración Electrónica, que tendrá voz y voto.

Todos los miembros del Comité tendrán un suplente. Los miembros del Comité y los respectivos suplentes serán designados por los titulares de los órganos superiores y directivos del Departamento y de los Organismos Públicos.

3. El Comité supervisará el cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, coordinará todas las actividades relacionadas con la seguridad de la información y ejercerá las siguientes funciones:

- a) Elaborar las propuestas de modificación y actualización permanente de la PSI del Ministerio de Fomento para su aprobación por la Comisión Ministerial de Administración Electrónica del Departamento.
- b) Impulsar el cumplimiento de la PSI y su desarrollo normativo según lo previsto en el artículo 12.b) de la presente Orden.
- c) Aprobar las normas de desarrollo de la PSI de segundo nivel, previstas en el artículo 12.b).
- d) Velar por el cumplimiento y difusión de la PSI, promoviendo actividades de concienciación y formación en materia de seguridad para el personal del Departamento.
- e) Coordinar las relaciones con el Comité de Seguridad de la Información de las Administraciones Públicas.
- f) Tomar aquellas decisiones que garanticen la seguridad de la información y de los servicios del Departamento.

4. El Comité se reunirá con carácter ordinario, al menos, anualmente. Por razones de urgencia podrá reunirse siempre que el Presidente lo estime conveniente.

El Comité podrá recabar del personal técnico propio o externo la información pertinente para la toma de sus decisiones, así como invitar a dicho personal a las reuniones con voz y sin voto.

El Comité de Seguridad de la Información ajustará su funcionamiento a las previsiones contenidas en el capítulo II del Título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, relativo a los órganos colegiados.

Artículo 6. *El Responsable de Seguridad.*

1. Conforme al artículo 10 del Real Decreto 3/2010, de 8 de enero, el Responsable de la Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

2. El Responsable de Seguridad del Ministerio de Fomento será el titular de la Subdirección General de Tecnologías de la Información y Administración Electrónica, desempeñando las siguientes funciones:

- a) Velar por la ejecución de las decisiones del Comité.
- b) Preparar los temas a tratar en las reuniones del Comité, realizar la convocatoria y elaborar el acta de las mismas; así como asesorar y darle soporte en cuantos asuntos estime de interés.
- c) Verificar que las medidas de seguridad son adecuadas para la protección de la información y de los servicios.
- d) Supervisar los sistemas de control interno, las evaluaciones periódicas de riesgos que se lleven a cabo en el Ministerio de Fomento y planificar las auditorías periódicas.
- e) Promover la concienciación, educación y formación en materia de seguridad de la información a todo el personal.
- f) Coordinar la investigación de incidentes de seguridad de la información.
- g) Proponer al Comité la normativa de seguridad de segundo nivel a la que se refiere el artículo 12.b).
- h) Asumir las funciones explícitamente atribuidas a la figura del Responsable de Seguridad en el Real Decreto 1720/2007, de 21 de diciembre de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad.

3. Cada uno de los órganos superiores y directivos Ministerio de Fomento y de los organismos autónomos y agencias estatales designarán una persona responsable que actuará como Responsable de Seguridad delegado y que servirá de apoyo al Responsable de Seguridad para el desarrollo de las tareas necesarias para la implantación de la PSI en sus respectivos ámbitos.

Artículo 7. *El Responsable de la Información.*

1. El Responsable de la Información es la persona que determina los requisitos de la información tratada, en el marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero, pudiendo solicitar una propuesta previa al Responsable de la Seguridad.

2. Esta responsabilidad recaerá sobre la persona titular de la Subdirección General o Unidad equivalente que gestione cada procedimiento administrativo.

Artículo 8. *El Responsable del Servicio.*

1. El Responsable del Servicio es la persona que determina los requisitos de los servicios prestados, en el marco establecido en el Anexo I del Real Decreto 3/2010, de 8 de enero, solicitando una propuesta al Responsable de la Seguridad.

2. Esta responsabilidad recaerá en titular de la Subdirección General o unidad administrativa equivalente que gestione cada servicio.

Artículo 9. *Resolución de conflictos.*

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

Artículo 10. *Formación y concienciación.*

1. El Ministerio de Fomento desarrollará actividades formativas específicas orientadas a la concienciación y formación de los empleados 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 Fomento.

Artículo 11. *Gestión de los riesgos.*

1. La gestión de riesgos para la seguridad de la información se realizará de manera continua sobre los sistemas de información, conforme con la legislación aplicable, incluidos los principios de gestión de la seguridad basada en los riesgos y reevaluación periódica, señalados en los artículos 6 y 9 del Real Decreto 3/2010, de 8 de enero.

2. Los Responsables de la Información y del Servicio son los encargados, de realizar el preceptivo análisis de riesgos. El Responsable de la Información deberá aprobar el nivel de riesgo residual, a propuesta del responsable del servicio. El Responsable de Seguridad recomendará un marco de directrices básicas para armonizar los criterios a seguir para la valoración de riesgos.

3. La selección de las medidas de seguridad a adoptar será propuesta por el personal de apoyo del Responsable de Seguridad en el órgano superior o directivo u organismo público correspondiente, y deberá ser aprobada por el Responsable de Seguridad.

4. El proceso de gestión de riesgos seguirá lo dispuesto en los anexos I y II del Real Decreto 3/2010, y deberá revisarse y aprobarse, al menos bienalmente, por cada responsable de la información y cada responsable de los servicios.

Artículo 12. *Desarrollo normativo de la Política de Seguridad de la Información.*

Las normas sobre seguridad de la Información en la Administración Electrónica del Departamento se clasificarán jerárquicamente en tres niveles, según su ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que todas se basarán en otra, u otras, de nivel superior.

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

b) Segundo nivel normativo: Normativa. Está constituido por la normativa de seguridad, en desarrollo de la PSI.

La normativa comprende los procedimientos y normas de seguridad de la información, de obligado cumplimiento, tras la aprobación por el Comité de Seguridad de la Información.

c) Tercer nivel normativo: Procedimientos Técnicos, en desarrollo del segundo nivel normativo, 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. Estos procedimientos establecen las configuraciones mínimas de seguridad de los diferentes elementos de un sistema de información, guías y recomendaciones de uso o de otro tipo.

El desarrollo de estos procedimientos técnicos de adaptación de la normativa será responsabilidad del personal de apoyo del Responsable de Seguridad en el órgano superior o directivo u organismo público correspondiente, y su aprobación será responsabilidad del Responsable de Seguridad.

Este marco documental estará a disposición de todos los miembros del Ministerio que necesiten conocerlo, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

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

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

Disposición adicional segunda. *Publicidad de la PSI.*

La presente orden se publicará en el «Boletín Oficial del Estado» y en la sede electrónica del Ministerio de Fomento.

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

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

Disposición final única. *Entrada en vigor.*

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

Madrid, 20 de octubre de 2014.–La Ministra de Fomento, Ana María Pastor Julián.