III. OTRAS DISPOSICIONES

MINISTERIO DE AGRICULTURA, ALIMENTACIÓN Y MEDIO AMBIENTE

5937 *Orden AAA/991/2015, de 21 de mayo, por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica del Ministerio de Agricultura, Alimentación y Medio Ambiente.*

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, establece la relación entre la Administración Pública y los ciudadanos a través de la Administración Electrónica, compuesta principalmente tanto por los sistemas de tecnologías de la información y comunicaciones como por el tratamiento y almacenamiento automatizado de la información que reside en los mismos, y determina, de acuerdo con su artículo 42, la aprobación del Esquema Nacional de Seguridad (ENS).

En efecto, esta consagración del derecho a comunicarse a través de medios electrónicos comporta la correlativa obligación de las Administraciones de atender a cuantas necesidades se adviertan para garantizar una aplicación segura de estas tecnologías sobre la base de los mandatos constitucionales de promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas y de remoción de los obstáculos que impidan o dificulten su plenitud.

En su desarrollo, se aprobaría 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, que tiene por objeto el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

El artículo 11 del citado real decreto exige que todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II de la propia norma (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica, y función diferenciada) y desarrollará una serie de requisitos mínimos consignados en el artículo 11.1.

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 (PSI) en el ámbito de la Administración Electrónica del Ministerio de Agricultura, Alimentación y Medio Ambiente.

2. La PSI será de obligado cumplimiento para todos los órganos superiores y directivos del Ministerio de Agricultura, Alimentación y Medio Ambiente, incluidos los organismos públicos vinculados o dependientes del Departamento, que no tengan establecida su propia política de seguridad. En aquellos organismos que tengan su propia política de seguridad, prevalecerá en caso de discrepancia la definida en esta orden ministerial.

3. La PSI será de obligado cumplimiento para todo el personal que acceda tanto a los sistemas de información como a la propia información que sea gestionada por el Departamento, con independencia de cuál sea su destino, adscripción o relación con el mismo.

cve: BOE-A-2015-5937
Verificable en http://www.boe.es

Artículo 2. *Principios de la seguridad de la información.*

1. Principios básicos.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Además de los previstos en el artículo 4 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, se establecen los siguientes:

a) Alcance estratégico: la seguridad de la información cuenta con el compromiso y apoyo de todos los niveles directivos de forma que está coordinada e integrada con el resto de iniciativas estratégicas del Departamento para conformar un todo coherente y eficaz.
b) Proporcionalidad: el establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
c) Mejora continua: las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
d) Seguridad por defecto: los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

2. Principios particulares y responsabilidades específicas.

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

a) Gestión de activos de información: los activos de información del Departamento se encontrarán inventariados y categorizados y estarán asociados a un responsable.
b) Seguridad ligada a las personas: se implantarán los mecanismos necesarios para que cualquier persona que acceda o pueda acceder a los activos de información conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.
c) Seguridad física: los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
d) Seguridad en la gestión de comunicaciones y operaciones: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las tecnologías de la información y comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
e) Control de acceso: se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
f) Adquisición, desarrollo y mantenimiento de los sistemas de información: se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

cve: BOE-A-2015-5937
Verificable en http://www.boe.es

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

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

i) Gestión de riesgos: debe realizarse de manera continua sobre los sistemas de información y contemplar un análisis de riesgos avanzado que evalúe los riesgos residuales y proponga tratamientos adecuados. Para la realización del análisis de riesgos se tendrán en cuenta las recomendaciones publicadas para el ámbito de la Administración Pública y en especial las guías elaboradas por el Centro Criptológico Nacional.

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

Artículo 3. *Estructura organizativa.*

La estructura organizativa para la gestión de la seguridad de la información en el ámbito descrito por la PSI del Ministerio de Agricultura, Alimentación y Medio Ambiente está compuesta por los siguientes agentes:

1. El Comité de Dirección de Seguridad de la Información, con un Comité Técnico.
2. Los Responsables de la Información.
3. Los Responsables del Servicio.
4. Los Responsables de Seguridad.
5. Los Responsables del Sistema.

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

1. Se crea el Comité de Dirección de Seguridad de la Información (CDSI), adscrito a la Subsecretaría del Ministerio de Agricultura, Alimentación y Medio Ambiente. El CDSI estará compuesto por los siguientes miembros:

a) Presidente: El titular de la Subsecretaría del Ministerio de Agricultura, Alimentación y Medio Ambiente.

b) Vicepresidente: El titular de la Dirección General de Servicios del Ministerio de Agricultura, Alimentación y Medio Ambiente.

c) Vocales, que deberán ser de nivel 30 o asimilado:

1.º Dos representantes de la Secretaría de Estado de Medio Ambiente, nombrados por el titular de dicho órgano superior.

2.º Dos representantes de la Subsecretaría, nombrados por el titular de dicho órgano superior.

3.º Un representante de la Secretaría General de Agricultura y Alimentación.

4.º Un representante de la Secretaría General de Pesca.

5.º Un representante de la Agencia Estatal de Meteorología (AEMET).

6.º Un representante del Fondo Español de Garantía Agrario (FEGA).

7.º Un representante del Organismo Autónomo Parques Nacionales (OAPN)

8.º El titular de la Subdirección General de Tecnologías de la Información y de las Comunicaciones, que actuará como Secretario, con voz y voto.

2. El CDSI ejercerá las siguientes funciones:

a) Elaborar las propuestas de modificación y actualización permanente que se hagan sobre la PSI.

b) Aprobar el resto de la normativa de seguridad de primer nivel definida en el artículo 9.

c) Velar e impulsar el cumplimiento de la PSI y de su desarrollo normativo.

d) Promover la mejora continua en la gestión de la seguridad de la información.

e) Aprobar el Plan de Auditoría y el Plan de Formación propuestos por el Responsable de Seguridad.

cve: BOE-A-2015-5937
Verificable en http://www.boe.es

f) Resolver los posibles conflictos que puedan derivarse del establecimiento de la citada estructura organizativa.

3. El CDSI se reunirá con carácter ordinario al menos una vez al año, y con carácter extraordinario cuando lo decida su Presidente.

Sin perjuicio de la celebración de dichas reuniones presenciales, de acuerdo con la autorización contenida en la disposición adicional primera de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, se faculta al Comité para que lleve a cabo las funciones que tiene asignadas por medios electrónicos, mediante votación por escrito y sin sesión presencial. En este caso, se remitirá a todos sus miembros, por vía electrónica y en un plazo máximo de siete días desde que reciba la petición de informe, el punto o puntos del día a discutir y la documentación correspondiente, dando un plazo mínimo de siete días y máximo de quince para que manifiesten por la misma vía su posición, voluntad u opinión.

En las actas que se levantaren para constancia de estas reuniones se incorporarán las comunicaciones que hayan tenido lugar, tanto para la convocatoria como para las deliberaciones y la adopción de decisiones.

4. El CDSI podrá recabar de personal técnico, propio o externo, la información pertinente para la toma de sus decisiones.

5. Los acuerdos se adoptarán por mayoría de los miembros. En caso de empate, el voto del presidente será dirimente.

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

1. Con carácter permanente se crea en el seno de la CDSI el Comité Técnico de Seguridad de la Información (CTSI), competente para conocer las cuestiones técnicas que deban de abordarse en relación con la PSI y con el fin de asegurar la coordinación en materia de seguridad de la información con el conjunto del Departamento y con otras instancias de la Administración General del Estado.

2. El CTSI estará compuesto por los siguientes miembros:

a) Presidencia: el Subdirector General de Tecnologías de la Información y de las Comunicaciones.

b) Vicepresidencia: el Subdirector General Adjunto de Tecnologías de la Información y de las Comunicaciones.

c) Vocalías: Serán los Responsables de Seguridad definidos en el artículo 7.

d) Secretaría: Un funcionario de al menos nivel 26, perteneciente a la Subdirección General de Sistemas Informáticos y Comunicaciones, tendrá voz pero no voto.

3. El CTSI colaborará con el CDSI en las cuestiones que éste le encomiende y, de forma particular, le corresponderá:

a) Elaborar estudios, análisis previos y propuestas de modificación y actualización de la PSI.

b) Elaborar estudios, análisis previos y propuestas sobre la normativa de seguridad de segundo y tercer nivel definida en el artículo 9.

c) Analizar el cumplimiento de la PSI y de su desarrollo normativo.

d) Analizar las medidas de seguridad de la información y de los servicios electrónicos prestados por los sistemas de información.

e) Estudiar las actividades de concienciación y formación en materia de seguridad.

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

g) Seguimiento de las medidas resultado del Análisis y gestión de riesgos de los activos.

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

cve: BOE-A-2015-5937
Verificable en http://www.boe.es

Sin perjuicio de la celebración de dichas reuniones presenciales, de acuerdo con la autorización contenida en la disposición adicional primera de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, se faculta al Comité para que lleve a cabo las funciones que tiene asignadas por medios electrónicos, mediante votación por escrito y sin sesión presencial. En este caso, se remitirá a todos sus miembros, por vía electrónica y en un plazo máximo de siete días desde que reciba la petición de informe, el punto o puntos del día a discutir y la documentación correspondiente, dando un plazo mínimo de siete días y máximo de quince para que manifiesten por la misma vía su posición, voluntad u opinión.

En las actas que se levantaren para constancia de estas reuniones se incorporarán las comunicaciones que hayan tenido lugar, tanto para la convocatoria como para las deliberaciones y la adopción de decisiones.

5. Los acuerdos se adoptarán por mayoría de los miembros. En caso de empate, el voto del presidente será dirimente.

Artículo 6. *Los responsables de la información y los responsables del servicio.*

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

2. Cada órgano superior o directivo del Ministerio de Agricultura, Alimentación y Medio Ambiente así como cada organismo público dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI, designará estos perfiles de acuerdo con su propia organización interna, sin que ello implique, en ningún caso, aumento de las dotaciones ni las retribuciones de dichos efectivos.

Artículo 7. *Los responsables de seguridad.*

1. Conforme al artículo 10 del Real Decreto 3/2010, de 8 de enero, el responsable de seguridad es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Cada órgano superior o directivo del Ministerio de Agricultura, Alimentación y Medio Ambiente así como cada organismo público vinculado o dependiente del Departamento a los que sea de aplicación la presente PSI designará un Responsable de Seguridad, sin que ello implique, en ningún caso, aumento de las dotaciones ni las retribuciones de dichos efectivos.

2. El ámbito de actuación de cada responsable de seguridad se limitará única y exclusivamente a los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean competencia y responsabilidad directa del centro al que pertenezca dicho responsable de seguridad.

3. Serán funciones de cada responsable de seguridad, dentro del ámbito de actuación enunciado en el punto anterior, las siguientes:

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

b) Elaborar la normativa de seguridad de segundo y tercer nivel definida en el artículo 9 y velar e impulsar su cumplimiento por parte de Responsables del Sistema del artículo 8 y de cualquier otro agente del sistema.

c) Encargarse de que la documentación de seguridad se mantenga organizada y actualizada, y de gestionar los mecanismos de acceso a la misma.

d) Promover la mejora continua en la gestión de la seguridad de la información.

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

cve: BOE-A-2015-5937
Verificable en http://www.boe.es

Artículo 8. *Los responsables del sistema.*

1. El responsable del sistema es la persona cuya responsabilidad es desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

2. Cada órgano superior o directivo del Ministerio de Agricultura, Alimentación y Medio Ambiente así como cada organismo público vinculado o dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI, designará este perfil, sin que ello implique, en ningún caso, aumento de las dotaciones ni las retribuciones de dichos efectivos.

Artículo 9. *Estructura de prescripciones sobre seguridad de la información.*

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

a) Primer nivel: constituido por la PSI y las directrices generales de seguridad aplicables a los órganos superiores o directivos del Ministerio de Agricultura, Alimentación y Medio Ambiente a los que, conforme al artículo 1, sea de aplicación la presente PSI.

b) Segundo nivel: constituido por las normas de seguridad desarrolladas por cada órgano superior o directivo del Ministerio de Agricultura, Alimentación y Medio Ambiente así como por cada organismo público dependiente del Departamento a los que, conforme al artículo 1, les sea de aplicación la presente PSI.

c) Tercer nivel: Procedimientos, guías e instrucciones técnicas complementarias. Son documentos que, cumpliendo con lo expuesto en la PSI, determinan las acciones o tareas a realizar en el desempeño de un proceso.

2. Tanto el segundo como el tercer nivel deberán:

a) Limitarse única y exclusivamente al ámbito específico de las competencias de cada uno de dichos órganos u organismos adscritos a la presente PSI. Este ámbito vendrá determinado por los sistemas de información y servicios de tecnologías de la información y de las comunicaciones que sean prestados y gestionados directamente por dicho órgano u organismo.

b) Cumplir estrictamente con lo indicado en el ENS y con el primer y segundo nivel normativos enunciados en el presente artículo.

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

3. Además de los elementos de obligado cumplimiento enunciados en el apartado 1, se podrá disponer, a criterio de cada uno de los órganos u organismos adscritos a la presente PSI, y siempre dentro del ámbito de sus competencias y responsabilidades, de otros documentos tales como estándares de seguridad, buenas prácticas, informes técnicos, etc.

4. El personal de cada uno de los órganos u organismos adscritos a la presente PSI tendrá la obligación de conocer y cumplir, además de la presente PSI, todas las directrices generales, normas y procedimientos de seguridad de la información que puedan afectar a sus funciones.

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

Las medidas descritas en esta orden no supondrán incremento del gasto, siendo atendidas con los medios materiales y humanos de que dispone el Ministerio de Agricultura, Alimentación y Medio Ambiente.

Asimismo, la asistencia a las reuniones no dará lugar a indemnización, remuneración o pago de ninguna clase.

cve: BOE-A-2015-5937
Verificable en http://www.boe.es

Disposición adicional segunda. *Deber de colaboración en la implantación de la PSI.*

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

Disposición adicional tercera. *Normativa supletoria.*

Los órganos previstos en esta orden se regirán, en todo lo demás, por lo previsto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

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

1. La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».
2. Esta orden se publicará en las sedes electrónicas del Ministerio de Agricultura, Alimentación y Medio Ambiente en cuyo ámbito sea de aplicación.

Madrid, 21 de mayo de 2015.–La Ministra de Agricultura, Alimentación y Medio Ambiente, Isabel García Tejerina.

cve: BOE-A-2015-5937
Verificable en http://www.boe.es