# III. OTRAS DISPOSICIONES

## MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

**9544** *Orden AEC/1647/2013, de 5 de septiembre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Asuntos Exteriores y de Cooperación.*

El desarrollo de la Administración Electrónica implica el tratamiento automatizado de gran cantidad de información, así como su almacenamiento por sistemas basados en tecnologías de la información y de las comunicaciones. Estos sistemas están expuestos a amenazas que aprovechándose de sus posibles vulnerabilidades pueden poner en peligro la información que manejan.

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 autenticidad, confidencialidad, integridad y disponibilidad de los datos almacenados o transmitidos y la de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (en adelante, 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 respectivas especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a conocimiento de personas no autorizadas.

Para ello, ENS enuncia en sus artículos del 5 al 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 (en adelante, PSI).

La PSI es, según ENS, el documento que define lo que significa seguridad de la información en una organización determinada, rige la forma en que dicha organización gestiona y protege la información y los servicios que considera críticos y debe plasmarse en un documento, accesible y comprensible para todos los miembros de la organización.

En concreto ENS dispone que:

1. 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 (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. La PSI deberá plasmarse en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

a) Los objetivos o misión de la organización.
b) El marco legal y regulatorio en el que se desarrollan sus actividades.
c) Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
d) La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

cve: BOE-A-2013-9544

4. La PSI debe ser coherente, en lo que proceda, con el correspondiente Documento de Seguridad, previsto en 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 la protección de datos de carácter personal en caso de discrepancias.

Para la elaboración de la PSI se han tenido en cuenta las guías CCN-STIC elaboradas por el Centro Criptológico Nacional (en adelante, CCN), en ejercicio de la función señalada en el artículo 2.2.a) del Real Decreto 421/2004, de 12 de marzo, que establecen las pautas de carácter general relativas a la organización de la seguridad y sus responsables, así como sobre la estructura y contenido mínimo de la PSI.

En virtud de lo anterior y en cumplimiento del artículo 11 del Real Decreto 3/2010, de 8 de enero, 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 Asuntos Exteriores y de Cooperación (en adelante, MAEC) y establecer el marco organizativo y tecnológico de la misma.

2. La PSI se aplicará por todos los órganos y unidades del Departamento y sus organismos adscritos, a todos los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias, debiendo ser cumplida por su personal y por cualquiera que tenga acceso a dichos datos, informaciones o servicios.

3. Las competencias asignadas por esta orden se ejercerán sin perjuicio de la competencia sobre seguridad de la información que atribuye a la Dirección General del Servicio Exterior el artículo 14.1.f) del Real Decreto 342/2012, de 10 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Exteriores y de Cooperación.

Artículo 2. *Misión del departamento.*

Corresponde al Ministerio de Asuntos Exteriores y de Cooperación, conforme a lo establecido en el Real Decreto 342/2012, de 10 de febrero, planificar, dirigir, ejecutar y evaluar la política exterior del Estado y la política de cooperación internacional para el desarrollo, con singular atención a las relacionadas con la Unión Europea y con Iberoamérica, y coordinar y supervisar todas las actuaciones que en dichos ámbitos realicen, en ejecución de sus respectivas competencias, los restantes Departamentos y Administraciones Públicas. Asimismo, le corresponde fomentar las relaciones económicas, culturales y científicas internacionales; participar, en la esfera de actuación que le es propia, en la propuesta y aplicación de las políticas migratorias y de extranjería; fomentar la cooperación transfronteriza e interterritorial; proteger a los españoles en el exterior; y preparar, negociar y tramitar los Tratados Internacionales de los que España sea parte.

Artículo 3. *Marco normativo.*

El marco normativo de las actividades del MAEC está integrado por las siguientes normas y la legislación sectorial reguladora de sus órganos superiores y directivos y organismos adscritos:

a) Ley 30/1992, de 26 de noviembre, de Régimen Jurídico Administrativo de las Administraciones Públicas y del Procedimiento Administrativo Común.

b) Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

cve: BOE-A-2013-9544

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

d) 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.

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

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

g) Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio.

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

i) 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.

j) 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.

k) Real Decreto 342/2012, de 10 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Exteriores y de Cooperación.

l) Orden AEC/2629/2010, de 7 de octubre, por la que se crea y regula el Registro Electrónico del Ministerio de Asuntos Exteriores y de Cooperación.

m) Orden AEC/2630/2010, de 7 de octubre, por la que se crea la Sede Electrónica del Ministerio de Asuntos Exteriores y de Cooperación.

n) Orden AEC/2703/2010, de 13 de septiembre, de creación y modificación de los ficheros de carácter personal del Ministerio de Asuntos Exteriores y de Cooperación.

o) Normas aplicables a la Administración Electrónica del Departamento derivadas y de inferior rango que las citadas en las letras anteriores, publicadas en las sedes electrónicas comprendidas en el ámbito de aplicación de la PSI.

También formarán parte del marco normativo las nuevas normas aplicables a la Administración Electrónica que afecten a la presente política de seguridad de la información.

Artículo 4. *Estructura organizativa de la política de seguridad de la información.*

La estructura organizativa de gestión de la seguridad de la información en el ámbito de la Administración Electrónica del Ministerio de Asuntos Exteriores y de Cooperación estará integrada por los siguientes agentes:

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

Artículo 5. *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). El Comité se configura como un grupo de trabajo en el seno de la Comisión Ministerial de Administración Electrónica del Departamento.

2. Composición. El Comité estará compuesto por:

a) Presidente: El Subsecretario de Asuntos Exteriores y de Cooperación.
b) Vicepresidente: El Director general del Servicio Exterior.
c) Vocales: En representación de los siguientes órganos del Departamento y de los organismos adscritos al Ministerio designados, a propuesta de sus titulares, por el Subsecretario de Asuntos Exteriores y de Cooperación y con nivel orgánico de subdirector general o asimilado los siguientes:

cve: BOE-A-2013-9544

Un Vocal representante del Gabinete del Ministro de Asuntos Exteriores y de Cooperación.
Un Vocal representante de la Secretaría de Estado de Asuntos Exteriores.
Un Vocal representante de la Secretaría de Estado para la Unión Europea.
Un Vocal representante de la Secretaría de Estado de Cooperación Internacional y para Iberoamérica.
Un Vocal representante de la Subsecretaría de Asuntos Exteriores y de Cooperación.
Un Vocal representante de la Dirección General de Españoles en el Exterior y Asuntos Consulares y Migratorios.
Un Vocal representante de la Dirección General de la Oficina de Información Diplomática.
Un Vocal representante de la Agencia Española de Cooperación Internacional para el Desarrollo.
Un Vocal representante del Instituto Cervantes.

d) Secretario. La persona titular de la Subdirección General de Informática, Comunicaciones y Redes, con voz y voto. En caso de ausencia, vacante o enfermedad ejercerá sus funciones el Subdirector general adjunto de Telecomunicaciones y Protección de la Información.

3. Expertos. El presidente podrá invitar a las reuniones del Comité a representantes de otras unidades o expertos cuando los asuntos a tratar lo requieran, así como recabar dictámenes e informes sobre dichos asuntos.
4. Funciones:

a) Elaborar las propuestas de modificación y actualización permanente de la PSI.
b) Aprobar las normas de desarrollo de la PSI de segundo nivel.
c) Velar por el cumplimiento y difusión de la PSI, promoviendo las actividades de concienciación y formación en materia de seguridad para el personal del Departamento.
d) Fijar las condiciones para satisfacer los requisitos de seguridad de la información y de los servicios.
e) Establecer directrices para coordinar la comunicación con el Centro Criptológico Nacional (en adelante, CCN) en la utilización de servicios de respuesta a incidentes de seguridad en la Administración Electrónica del Departamento.
f) Informar sobre el estado de las principales variables de seguridad en los sistemas de información del Departamento al Comité de Seguridad de la Información de las Administraciones Públicas, con objeto de elaborar un perfil general del estado de dichas variables.
g) Compartir entre sus miembros experiencias de éxito en materia de seguridad para velar por el cumplimiento de la PSI y su normativa de desarrollo.
h) Tomar todas aquellas decisiones que garanticen la seguridad de la información y servicios del Departamento.

5. Reuniones. El Comité se reunirá, al menos, con periodicidad anual.

Artículo 6. *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, 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.
3. Las funciones de cada Responsable de la Información, dentro de su ámbito de actuación, son las siguientes:

cve: BOE-A-2013-9544

a) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información, conforme con lo establecido en el artículo 44 del Real Decreto 3/2010, de 8 de enero.

b) Son los encargados, junto a los Responsables del Servicio y contando con la participación del Responsable de Seguridad, de realizar los preceptivos análisis de riesgos, y seleccionar las salvaguardas que se han de implantar.

c) Son los responsables de aceptar los riesgos residuales respecto de la información calculados en el análisis de riesgos.

d) Son los responsables de realizar el seguimiento y control de los riesgos, con la participación del Responsable de Seguridad.

Artículo 7. *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 o unidad administrativa que gestione cada servicio.

3. Las funciones de cada Responsable del Servicio, dentro de su ámbito de actuación, son las siguientes:

a) Son los encargados, junto a los Responsables de la Información y contando con la participación y asesoramiento del Responsable de Seguridad, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas que se han de implantar.

b) Son los responsables de aceptar los riesgos residuales respecto a los servicios calculados en el análisis de riesgos.

c) Son los responsables de realizar el seguimiento y control de los riesgos con la participación del Responsable de Seguridad.

d) Suspender, de acuerdo con el Responsable de la Información y el Responsable de Seguridad, la prestación de un servicio electrónico o el manejo de una determinada información, si es informado de deficiencias graves de seguridad.

Artículo 8. *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. Se designarán los siguientes Responsables de Seguridad, según su ámbito de responsabilidad:

a) Responsable de Seguridad cuyo ámbito de responsabilidad comprende la información y servicios afectados por los sistemas de información gestionados por la Subsecretaría de Asuntos Exteriores y de Cooperación. Corresponderá al Grupo técnico al que se refiere el punto 3 del presente artículo.

b) Responsable de Seguridad cuyo ámbito de responsabilidad comprende la información y servicios afectados por aquellos sistemas de información gestionados por la Secretaría de Estado de la Unión Europea. La designación corresponderá al titular de la Secretaría de Estado de la Unión Europea.

c) Responsable de Seguridad en la Agencia Española de Cooperación Internacional para el Desarrollo. La designación corresponderá al titular de la Dirección de la Agencia Española de Cooperación Internacional para el Desarrollo.

d) Responsable de Seguridad en el Instituto Cervantes. La designación corresponderá al titular de la Dirección del Instituto Cervantes.

3. El Grupo técnico responsable de seguridad del ámbito de la Subsecretaría de Asuntos Exteriores y de Cooperación estará coordinado por el titular de la Subdirección

cve: BOE-A-2013-9544

General de Informática, Comunicaciones y Redes y compuesto por un representante de cada uno los siguientes órganos designados por los titulares de aquéllos:

Inspección General de Servicios.
Oficialía Mayor.
Subdirección General de Personal.
El Subdirector General Adjunto de Telecomunicaciones y Protección de la Información, que ejercerá las funciones de Secretario y coordinará al Equipo de seguridad.

4. Funciones del Responsable de Seguridad.

a) Promover la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.
b) Proponer al Comité de Seguridad la normativa de seguridad de segundo nivel a la que se refiere el artículo 13 apartado b).
c) Aprobar la normativa de seguridad de tercer nivel a la se refiere el artículo 13 apartado c).
d) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
e) Realizar el seguimiento y control del estado de seguridad de los sistemas de información.
f) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.
g) Participar junto a los Responsables de la Información y a los Responsables del Servicio en la realización de los preceptivos análisis de riesgos.
h) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
i) Elaborar informes periódicos de seguridad para el Comité, que incluirán los incidentes más relevantes de cada periodo.

5. Cuando lo justifique la complejidad, la distribución o separación física de sus elementos o el número de usuarios de la información en soporte electrónico, o de los sistemas que la manejen, los responsables de seguridad podrán designar «responsables de seguridad delegados», dependientes funcionalmente de ellos y responsables en su ámbito de las actuaciones que se les deleguen.
6. En todos los casos, las designaciones a las que hace referencia el presente artículo se realizarán de entre los efectivos que presten servicios en el Departamento y sus organismos públicos adscritos.

Artículo 9. *Equipo de Seguridad.*

1. El Equipo de Seguridad es un grupo de apoyo al Responsable de Seguridad para el cumplimiento de sus funciones, que aglutinará los esfuerzos 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 de los sistemas y servicios (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. Los componentes del Equipo de Seguridad se determinarán por el Responsable de Seguridad, de entre los efectivos que presten servicios en el Departamento y sus organismos públicos adscritos.

cve: BOE-A-2013-9544

Artículo 10. *Resolución de conflictos.*

1. En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la PSI, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité para la Gestión y Coordinación de la Seguridad de la Información.
2. En la resolución de estas controversias prevalecerán las mayores exigencias derivadas de la protección de datos de carácter personal.

Artículo 11. *Obligaciones del personal.*

1. Todo el personal que presta servicios en el Ministerio de Asuntos Exteriores y de Cooperación y sus organismos adscritos, tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa de seguridad derivada, siendo responsabilidad del Comité disponer los medios necesarios para que la información llegue a los afectados.
2. Todo el personal que se incorpore al Ministerio de Asuntos Exteriores y de Cooperación o vaya a tener acceso a alguno de sus sistemas de información o la información gestionada por ellos deberá ser informado y deberá cumplir la Política de Seguridad de la Información y la normativa de seguridad derivada.
3. El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa de seguridad derivada podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades contractuales y legales correspondientes.

Artículo 12. *Gestión de riesgos.*

1. La gestión de riesgos para la seguridad de la información se realizará de manera continua sobre los sistemas de información y de los servicios, 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, con la participación del Responsable de Seguridad, de realizar el preceptivo análisis de riesgos, proponer las salvaguardas adecuadas y calcular el riesgo residual.
3. Las salvaguardas identificadas en el preceptivo análisis y gestión de riesgos serán aplicadas por la unidad competente de acuerdo al Real Decreto 342/2012, de 10 de febrero.
4. El Responsable de Seguridad velará por la correcta implementación de las salvaguardas y que éstas consiguen el efecto deseado.
5. Los riesgos sobre la información y sobre los servicios competen a los responsables de la Información y del Servicio, respectivamente, y por tanto éstos han de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control.
6. El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas de información, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, será revisado anualmente por el correspondiente responsable de seguridad, que elevará un informe al Comité.
7. Para realizar el análisis de riesgos se utilizará la metodología Magerit aprobada por el Consejo Superior de Administración Electrónica, y las herramientas que la apliquen, como PILAR desarrollada por el Centro Criptológico Nacional.

Artículo 13. *Clasificación y jerarquía del desarrollo normativo de la Política de Seguridad de la Información.*

1. Las normas del MAEC sobre seguridad de la información en la Administración Electrónica del Departamento se clasificarán jerárquicamente en tres niveles, según su

cve: BOE-A-2013-9544

ámbito de aplicación y grado de detalle técnico, de modo que todas se basarán en otra, u otras, de nivel superior:

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

b) Segundo nivel normativo: Normativa y recomendaciones de seguridad. Está constituido por la normativa y las recomendaciones de seguridad, en desarrollo de la PSI, que se definan para cada ámbito organizativo de aplicación específico. Dicho ámbito podrá corresponder a uno o más órganos superiores o directivos del MAEC u organismos públicos dependientes.

En cuanto a la normativa de seguridad de este segundo nivel, comprenderá la regulación de procedimientos sobre «Seguridad en las Tecnologías de la Información y las Comunicaciones» (en adelante, STIC), y normas e instrucciones técnicas STIC, dictadas, con la aprobación previa del Comité, por los titulares de los órganos superiores o directivos en cuyo ámbito se hayan de aplicar.

En cuanto a las recomendaciones, versarán sobre buenas prácticas y consejos no vinculantes para la mejora de las condiciones de seguridad de la información en soporte electrónico. Las recomendaciones las propone el Responsable de Seguridad, dentro de su ámbito de competencia, y las aprueba el Comité.

c) Tercer nivel normativo: Procesos y Procedimientos Técnicos. Corresponden al desarrollo del segundo nivel normativo. Está constituido por Procesos y Procedimientos que detallan los aspectos técnicos para realizar una determinada tarea respetando los principios de seguridad de la organización y los procesos internos en ella establecidos. Están orientados a resolver determinadas tareas, consideradas críticas por el perjuicio que causaría su gestión inadecuada. Incluyen aspectos de configuración, implementación y tecnológicos relativos a la seguridad, desarrollo, mantenimiento y explotación de los sistemas de información. Su ámbito de aplicación podrá ser general o corresponder a un ámbito orgánico específico o un sistema de información determinado.

Se incluyen en este nivel normativo las guías CCN-STIC.

La aprobación de los Procedimientos técnicos corresponde al Responsable de Seguridad.

2. El Comité establecerá mecanismos para compartir la documentación derivada del desarrollo normativo de la PSI, con objeto de estandarizar en la medida de lo posible dicho desarrollo en su ámbito de aplicación.

Artículo 14. *Responsables de datos de carácter personal.*

1. En lo que se refiere a los ficheros con datos de carácter personal, estarán referenciados en el correspondiente documento de seguridad donde se hará constar tanto los ficheros afectados como los responsables correspondientes.

2. Todos los sistemas de información del Ministerio de Asuntos Exteriores y de Cooperación se ajustarán a los niveles de seguridad requeridos por la normativa de protección de datos de carácter personal. En caso de conflicto con la normativa de seguridad indicada en el artículo 13 prevalecerá la norma que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal.

Artículo 15. *Formación y concienciación.*

1. Con la colaboración, en su caso, del CCN, se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos del Departamento, así como a la difusión entre ellos 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 MAEC.

cve: BOE-A-2013-9544

Artículo 16. *Actualización permanente y revisiones.*

1. La PSI se deberá actualizar permanentemente para adecuarla al progreso de los servicios de Administración Electrónica, la evolución tecnológica, el desarrollo de la sociedad de la información, y 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 Subsecretaría de Asuntos Exteriores y de Cooperación, produciendo efectos a partir del día siguiente de su publicación en la sede electrónica del Departamento.

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

La aplicación de esta orden no conllevará incremento de 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, 5 de septiembre de 2013.–El Ministro de Asuntos Exteriores y de Cooperación, José Manuel García-Margallo y Marfil.

cve: BOE-A-2013-9544