III. OTRAS DISPOSICIONES

MINISTERIO DEL INTERIOR

12468 *Orden INT/2213/2013, de 19 de noviembre, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio del Interior.*

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, señala entre sus fines el 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 artículo 42 de la citada Ley 11/2007, de 22 de junio, vino a contemplar el Esquema Nacional de Seguridad (ENS), cuyo objeto es 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.

En cumplimiento de dicha Ley, el Real Decreto 3/2010, de 8 de enero, reguló el ENS en el ámbito de la administración electrónica, con el fin de fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán 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 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 de 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, disponiendo 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.
2. La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.
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 la documentación de seguridad del sistema, su gestión y acceso.
4. Además, la PSI debe ser 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 el Real Decreto 1720/2007, de 21 de diciembre, 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 son una referencia las guías CCN-STIC, principalmente 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

cve: BOE-A-2013-12468

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

Esta orden ministerial ha sido informada por la Comisión Ministerial de Administración Electrónica y por el Consejo Superior de Administración Electrónica.

En su virtud, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. El objeto de la presente orden es la aprobación de la Política de Seguridad de la Información (en adelante, PSI) en el ámbito de la administración electrónica del Ministerio del Interior, así como el establecimiento del marco organizativo y tecnológico de la misma.

La PSI se desarrollará posteriormente en otros niveles normativos, en los que se detallarán los aspectos particulares involucrados en la gestión de la seguridad de los sistemas de información que soportan los servicios electrónicos prestados por el Ministerio del Interior a los ciudadanos con los que se relaciona.

2. Se aplicarán los principios básicos y los requisitos mínimos que se establecen en 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, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, que permita una protección adecuada de la información y los servicios.

3. La PSI será de aplicación a los sistemas de información y activos utilizados por el Ministerio del Interior en la prestación de los servicios de administración electrónica, en el marco de sus competencias. Asimismo, la PSI deberá ser de obligado cumplimiento por todo el personal con acceso a los sistemas de información del citado Departamento, con independencia de cuál sea su destino, adscripción o relación con el mismo.

4. Por otra parte, será de obligado cumplimiento para todos los órganos y unidades del Ministerio del Interior, así como para los organismos públicos dependientes del mismo.

5. Se faculta a los Centros Directivos para que, en el ámbito de sus competencias, amplíen de manera progresiva el ámbito de aplicación de la PSI a los sistemas de información no relacionados con la administración electrónica.

Artículo 2. *Misión del Departamento.*

Corresponde al Ministerio del Interior lo previsto en el Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del mismo.

Artículo 3. *Marco normativo.*

1. El marco normativo en que se desarrollan las actividades del Ministerio del Interior comprende la legislación sectorial reguladora de la actuación de los órganos superiores y directivos del mismo y de sus organismos públicos adscritos, así como la normativa en vigor correspondiente a la administración electrónica.

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 PSI en el Ministerio del Interior está compuesta por los siguientes agentes:

a) El Comité Superior para la Seguridad de la Información.
b) Los Grupos de Trabajo para la Seguridad de la Información.
c) El Grupo de Trabajo de los Responsables de la Seguridad.
d) El Responsable de la Información.
e) El Responsable del Servicio.

cve: BOE-A-2013-12468

f) El Responsable de la Seguridad.
g) El Responsable del Sistema.

Artículo 5. *El Comité Superior para la Seguridad de la Información.*

1. Se crea el Comité Superior para la Seguridad de la Información (en adelante, CSSI), configurado como un grupo de trabajo en el seno de la Comisión Ministerial de Administración Electrónica del Departamento, será el encargado de coordinar todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito del Ministerio del Interior, y ejercerá las siguientes funciones:

a) Aprobar las propuestas de modificación y actualización permanente de la PSI.
b) Velar e impulsar el cumplimiento de la PSI, así como su desarrollo normativo.
c) 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.
d) Promover la mejora continua en la gestión de la seguridad de la información.
e) Impulsar la formación y concienciación.
f) Resolver los conflictos que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

2. El CSSI está compuesto por los siguientes miembros, que podrán ser sustituidos por un suplente con categoría mínima de Subdirector General o asimilado:

a) Presidente: Titular de la Subsecretaría del Ministerio del Interior.
b) Vicepresidente: Titular de la Secretaría General Técnica.
c) Vocales: Titulares de los siguientes Centros Directivos:

i. Dirección General de la Policía.
ii. Dirección General de la Guardia Civil.
iii. Secretaría General de Instituciones Penitenciarias.
iv. Dirección General de Relaciones Internacionales y Extranjería.
v. Dirección General de Política Interior.
vi. Dirección General de Tráfico.
vii. Dirección General de Protección Civil y Emergencias.
viii. Dirección General de Apoyo a Víctimas del Terrorismo.
ix. Gabinete del Secretario de Estado de Seguridad.

d) Secretario: con voz y voto, el Subdirector General de Tecnologías de la Información y las Comunicaciones de la Subsecretaría, que será el garante de la ejecución directa o delegada de las decisiones del CSSI. Se encarga de preparar los temas a tratar en las reuniones, realizar la convocatoria y elaborar el acta de las mismas.

3. El CSSI se reunirá con carácter ordinario, al menos, una vez al año. Por razones de urgencia podrá reunirse siempre que la Presidencia lo estime conveniente.
4. En las reuniones del CSSI podrán participar cuantos asesores, internos o externos, se estime conveniente por parte de la Presidencia del mismo.

Artículo 6. *Los Grupos de Trabajo para la Seguridad de la Información.*

1. Se crea un Grupo de Trabajo para la Seguridad de la Información (en adelante, GTSI) por cada uno de los siguientes Centros Directivos del Ministerio del Interior, con competencias en gestión de tecnologías de la información:

a) Secretaría de Estado de Seguridad.
b) Subsecretaría del Interior.
c) Dirección General de la Policía.

cve: BOE-A-2013-12468

d) Dirección General de la Guardia Civil.
e) Secretaría General de Instituciones Penitenciarias.
f) Dirección General de Tráfico.
g) Dirección General de Protección Civil y Emergencias.
h) Organismo Autónomo Trabajo Penitenciario y Formación para el Empleo.

2. El GTSI ejercerá las siguientes funciones, que podrán ser ampliadas dentro su ámbito competencial:

a) Redactar y aprobar las normas de segundo nivel correspondientes al ámbito de influencia de su Centro Directivo.
b) Velar e impulsar el cumplimiento de las normas de segundo nivel y promover el desarrollo del tercer nivel normativo.
c) Aprobación de documentos de correspondencia de responsables en su ámbito competencial, detallados de acuerdo al ENS, y la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
d) Aprobación de los planes de mejora de la seguridad en su ámbito de competencias, de acuerdo a los presupuestos disponibles.
e) Informar sobre el estado de las principales variables de seguridad de sus sistemas de información, para la elaboración de un perfil general del estado de seguridad del Ministerio.
f) Promover la mejora continua en la gestión de la seguridad de la información en su ámbito de competencias.
g) Impulsar la formación y concienciación en su ámbito.
h) Resolver los conflictos que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

3. La composición final y funcionamiento de cada GTSI será determinada por el titular del Centro Directivo de entre los funcionarios adscritos al mismo adecuándose a la estructura del Centro Directivo. Estará compuesto, al menos, por los siguientes miembros:

a) Responsable de la Información.
b) Responsable del Servicio.
c) Responsable de la Seguridad
d) Responsable de Sistemas

Por cada Centro Directivo podrán designarse uno o varios Responsables de la Información, uno o varios Responsables de los Servicios, y uno o varios Responsables de Sistemas, de acuerdo a la Organización del Centro Directivo, siendo los mismos titulares de las Unidades Administrativas competentes en la gestión de la información, los servicios y los sistemas informáticos, respectivamente, respecto al ámbito y objeto de la presente Orden. Dichas funciones podrán ser encomendadas a personal funcionario de la correspondiente Unidad Administrativa.

La designación del responsable de la Seguridad en cada Centro Directivo la realizará el titular del mismo, y será coherente con las estructuras organizativas existentes en relación con la Seguridad de la Información y acorde con las funciones que desempeñan en su puesto de trabajo habitual.

Artículo 7. *El Grupo de Trabajo de Responsables de la Seguridad.*

1. Se crea un Grupo de Trabajo de Responsables de la Seguridad (en adelante, GTRS), bajo dependencia directa del CSSI.
2. Las funciones del GTRS son:

a) Elaborar las propuestas de modificación y actualización permanente de la PSI, y someterlas a la aprobación del CSSI.

cve: BOE-A-2013-12468

b) Asegurar la coherencia de las políticas de seguridad sectoriales que afecten al Departamento.

c) Elaboración del perfil general del estado de seguridad del Ministerio, integrando el estado de las principales variables de seguridad de cada Centro Directivo para someterlo al CSSI.

d) Coordinar la comunicación del Departamento con el Centro Criptológico Nacional (CCN) en la utilización de servicios de respuesta a incidentes de seguridad, sin perjuicio de las comunicaciones que, en su ámbito competencial, se realicen por el Responsable de la Seguridad de cada GTSI.

e) Colaboración en la investigación y resolución de incidentes de seguridad de la información, tanto en el ámbito interno como externo al Departamento.

3. El GTRS está compuesto por los siguientes miembros:

a) Presidente: El Subdirector General de Tecnologías de la Información y las Comunicaciones.

b) Vocales: El responsable de la Seguridad de cada Centro Directivo.

c) Secretario: Un funcionario de la Subdirección General de Tecnologías de la Información y las Comunicaciones.

4. En las reuniones del GTRS podrán participar cuantos asesores, internos o externos, estimen necesarios los miembros del mismo.

5. El GTRS se reunirá con carácter ordinario, al menos, trimestralmente. Por razones de urgencia podrá reunirse siempre que la Presidencia lo estime conveniente.

Artículo 8. *El Responsable de la Información.*

1. Conforme a los artículos 10 y 44 del Real Decreto 3/2010, de 8 de enero, el Responsable de la Información es la persona u órgano corporativo que tiene la potestad de establecer los requisitos de la información en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de la información.

2. Serán funciones del Responsable de la Información, dentro de su ámbito de actuación, las siguientes:

a) Determinar los niveles de seguridad de la información tratada, valorando los impactos de los incidentes que afecten a la seguridad de la información.

b) Son los encargados, junto a los Responsables del Servicio y contando con la participación del Responsable de la 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) Para la determinación de los niveles de seguridad de la información, el Responsable de la Información solicitará informe del Responsable de la Seguridad.

Artículo 9. *El Responsable del Servicio.*

1. Conforme al artículo 10 del Real Decreto 3/2010, de 8 de enero, el Responsable del Servicio es la persona u órgano corporativo que tiene la potestad de establecer los requisitos del servicio en materia de seguridad. Es el encargado de determinar los niveles de seguridad del servicio en cada dimensión de seguridad, dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero.

2. Serán funciones del Responsable del Servicio, dentro de su ámbito de actuación, las siguientes:

a) Determinar los niveles de seguridad del servicio, valorando los impactos de los incidentes que afecten a la seguridad del servicio.

cve: BOE-A-2013-12468

b) Son los encargados, junto a los Responsables de la Información y contando con la participación del responsable de la 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 los servicios calculados en el análisis de riesgos.

d) Para la determinación de los niveles de seguridad del servicio, el Responsable del Servicio solicitará informe del Responsable de la Seguridad.

3. Podrá coincidir en la misma persona u órgano las responsabilidades de la información y del servicio. La diferenciación tendrá lugar cuando el servicio maneja información de distintas procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio cuando dicha prestación no depende de la unidad que es Responsable de la Información.

Artículo 10. *El Responsable de la Seguridad.*

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

2. Serán funciones del Responsable de la Seguridad, dentro de su ámbito de actuación, las siguientes:

a) Desarrollar las directrices, estrategias y objetivos dictados por el GTSI.

b) Proveer de asesoramiento y apoyo al GTSI.

c) Elaborar la normativa de seguridad.

d) Aprobar los procedimientos operativos de seguridad.

e) Mantener la seguridad de la información manejada y de los servicios electrónicos prestados por los sistemas de información.

f) Realizar o promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.

g) Realizar el seguimiento y control del estado de seguridad del sistema de información.

h) Verificar que las medidas de seguridad son adecuadas para la protección de la información y los servicios.

i) Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

j) Elaborar informes periódicos de seguridad para el GTSI que incluyan los incidentes más relevantes de cada período.

k) Supervisar el registro de activos.

3. Por cada Centro Directivo se designará un Responsable de Seguridad entre los funcionarios del Centro. Cuando la complejidad, distribución, separación física de sus elementos o número de usuarios de los sistemas de información lo justifiquen, el titular del Centro Directivo podrá designar los responsables de la seguridad delegados que considere necesarios entre los funcionarios del Centro, que tendrán dependencia funcional directa del Responsable de la Seguridad y serán responsables en su ámbito de todas aquellas acciones que les delegue.

Artículo 11. *El Responsable del Sistema.*

1. El Responsable del Sistema es la persona que tiene la responsabilidad de desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

2. Son funciones del Responsable del Sistema:

a) Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

cve: BOE-A-2013-12468

b) Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

c) Posibilidad de acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y el Responsable de la Seguridad, antes de ser ejecutada.

Artículo 12. *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 CSSI.

Artículo 13. *Gestión de los 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 del Real Decreto 3/2010, de 8 de enero) y reevaluación periódica (artículo 9 del Real Decreto 3/2010, de 8 de enero).

2. Los Responsables de la Información y del Servicio son los responsables de los riesgos sobre la información y sobre los servicios, respectivamente, y por tanto, de aceptar los riesgos residuales calculados en el análisis, así como de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

3. La selección de las medidas de seguridad a aplicar será propuesta por cada Responsable de Seguridad al GTSI correspondiente.

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 proporcionales a los riesgos y estar justificadas, deberá revisarse cada año por parte del Responsable de Seguridad, que elevará un informe al GTSI correspondiente.

Artículo 14. *Desarrollo normativo de la PSI. Documentación de Seguridad.*

1. El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en tres niveles, según el ámbito de aplicación y nivel de detalle técnico, 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: Política de Seguridad de la Información y directrices y normas de seguridad generales para todo el Ministerio del Interior.

b) Segundo nivel normativo: Normas Específicas de Seguridad de la Información y Normas de Seguridad TIC (Normas STIC). Las mismas desarrollan y detallan la Política de Seguridad de la Información, centrándose en un área o aspecto determinado de la seguridad de la información.

c) Tercer nivel normativo: Procesos y Procedimientos STIC e Instrucciones Técnicas STIC. Son documentos que dan respuesta, incluyendo detalles de implementación y tecnológicos, a cómo se puede realizar una determinada tarea cumpliendo con lo expuesto en la PSI.

Los Procesos, Procedimientos STIC e Instrucciones Técnicas STIC de un determinado ámbito de actuación los aprueba el correspondiente Responsable de Seguridad.

2. Además de los documentos citados en el apartado 1, la documentación de seguridad del sistema podrá contar, bajo criterio del Responsable de Seguridad correspondiente, con otros documentos de carácter no vinculante: recomendaciones, buenas prácticas, informes, registros, evidencias electrónicas, etc.

3. Cada Responsable de Seguridad deberá mantener la documentación de seguridad actualizada y organizada, y gestionar los mecanismos de acceso a la misma.

cve: BOE-A-2013-12468

4. El GTSI 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 15. *Protección de datos de carácter personal.*

1. Los datos de carácter de personal que sean objeto de tratamiento en la prestación de los servicios de administración electrónica ofrecidos por el Ministerio del Interior, deberán protegerse mediante la implantación de las medidas de seguridad correspondientes, a tenor de lo dispuesto en:

a) El título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.
b) El anexo II del Real Decreto 3/2010, de 8 de enero.

2. En relación con los sistemas de información que, para soportar la prestación de servicios de administración electrónica, manejen datos de carácter personal, prevalecerán las mayores exigencias contenidas en el título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 16. *Terceras partes.*

1. Cuando el Ministerio del Interior utilice servicios o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
2. Cuando el Ministerio del Interior preste servicios o ceda información a terceros, se les hará partícipes de esta Política y de la Normativa de Seguridad que ataña a dichos servicios e información. Los mismos quedarán sujetos a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias y se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad.
3. Cuando algún aspecto de la PSI no pueda ser satisfecho por una tercera parte según se establece en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Dicho informe habrá de ser aprobado por los responsables de la información y los servicios afectados.

Artículo 17. *Concienciación y formación.*

Todo el personal relacionado con la información, los servicios y los sistemas de información, deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad de la información. Para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios del Ministerio del Interior, se articularán los mecanismos necesarios para llevar a la práctica la concienciación y la formación específica necesaria e imprescindible en todos los niveles de la organización.

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

Las medidas previstas en la presente orden serán atendidas con los medios materiales y humanos de que dispone el Ministerio del Interior, por lo que no supondrá incremento alguno del gasto público.

cve: BOE-A-2013-12468

Disposición final primera. *Publicidad de la PSI.*

La presente orden se publicará, además de en el «Boletín Oficial del Estado», en cada una de las sedes electrónicas del Ministerio del Interior.

Disposición final segunda. *Entrada en vigor.*

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

Madrid, 19 de noviembre de 2013.–El Ministro del Interior, Jorge Fernández Díaz.

cve: BOE-A-2013-12468