III. OTRAS DISPOSICIONES

MINISTERIO DEL INTERIOR

5536 *Orden INT/424/2019, de 10 de abril, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio del Interior y las directrices generales en materia de seguridad de la información para la difusión de resultados provisionales en procesos electorales.*

La 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, identifica responsabilidades y establece el conjunto de principios y directrices básicos para una protección apropiada y consistente de los servicios y activos de información gestionados en el marco de competencias del Ministerio, generando así, de acuerdo con lo establecido en 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, las condiciones necesarias de confianza en el uso de medios electrónicos.

Desde el año 2013, se ha asistido a la modificación del marco normativo básico de aplicación en el ámbito de la administración electrónica. Por un lado, la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones Públicas recoge en su artículo 13 entre los derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece en su artículo 3 sobre principios generales que las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados. Esta Ley, recoge expresamente en su artículo 156 el Esquema Nacional de Seguridad al regular, en su Título III Capítulo IV, las relaciones electrónicas entre las Administraciones.

La política de seguridad de la información vigente del Ministerio del Interior, en adelante PSI, establece la estructura organizativa de acuerdo con la estructura del mismo establecida por Real Decreto 400/2012, de 17 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio del Interior. Esta estructura, se ha visto modificada por normativa posterior y, especialmente por el Real Decreto 952/2018, de 27 de julio, que adecúa la estructura del departamento a las nuevas necesidades organizativas en aras de aumentar la eficacia de la actuación administrativa, en el ámbito de competencias del departamento, en un contexto de continua evolución tecnológica.

De acuerdo con este mismo Real Decreto 952/2018, de 27 de julio, el departamento asume la realización de las actuaciones necesarias para el desarrollo de los procesos electorales. Para ello, utiliza servicios, comunicaciones y sistemas informáticos que deben reunir las condiciones técnicas y de seguridad de la información adecuadas para garantizar el efectivo ejercicio del derecho fundamental a la participación política y, con ello, su imbricación con la propia legitimidad democrática de los resultados. En este sentido, la presente Orden tiene también como objetivo fortalecer la capacidad de identificación, detección, prevención, contención y adecuada gestión ante posibles ciberamenazas en el ámbito de los procesos electorales, coordinando actuaciones a través de la creación del Subcomité de Seguridad de la Información en Procesos electorales, adscrito al Comité Superior para la Seguridad de la Información.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

Asimismo, han entrado en vigor, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos); la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales; el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información; la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (pendiente de trasposición).

Continúa en vigor, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

Por todo ello, debe adaptarse la Política de Seguridad de la Información del Ministerio a los nuevos requerimientos normativos.

Esta orden cumple con los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia recogidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Se ha recabado informe de la Comisión Ministerial de Administración Digital del Ministerio del Interior y de la Agencia Española de Protección de Datos.

En virtud de lo anterior, con la aprobación previa de la Ministra de Política Territorial y Función Pública, dispongo:

Artículo 1. *Objeto.*

La presente orden tiene por objeto:

a) La creación del Subcomité de Seguridad de la Información para la Difusión de Resultados Provisionales en Procesos Electorales.

b) La actualización de la Política de Seguridad de la Información del Ministerio del Interior en el ámbito de la administración electrónica (en adelante, PSI), para adecuarla al marco jurídico actual, al progreso de los servicios de administración electrónica, a la evolución tecnológica y la consolidación de las infraestructuras que la apoyan.

c) La aprobación de las Directrices de Seguridad de la Información para la Difusión de Resultados Provisionales en materia de procesos electorales.

CAPÍTULO I

Política de seguridad de la información

Artículo 2. *Política de Seguridad de la Información.*

1. La PSI en el ámbito de la administración electrónica del Ministerio del Interior identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados en el ámbito de competencias del Ministerio del Interior, estableciendo el marco organizativo y tecnológico de la misma.

2. La PSI se desarrollará posteriormente en otros niveles normativos, de acuerdo con lo establecido en el artículo 18 de esta orden, en el que se detallarán los aspectos particulares involucrados en la gestión de la seguridad de los sistemas de información

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

que soportan los servicios electrónicos prestados por el Ministerio del Interior a los ciudadanos y personas jurídicas con los que se relaciona.

3. 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.

4. 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.

5. 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.

6. 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 3. *Misión del Departamento.*

Corresponde al Ministerio del Interior, de acuerdo con lo establecido en el Real Decreto 952/2018, de 27 de julio, por el que se desarrolla su estructura orgánica básica, la propuesta y ejecución de la política del Gobierno en materia de seguridad ciudadana; la promoción de las condiciones para el ejercicio de los derechos fundamentales, en particular la libertad y seguridad personales, en los términos establecidos en la Constitución Española y en las leyes que los desarrollen; el mando superior y la dirección y coordinación de las Fuerzas y Cuerpos de Seguridad del Estado; las competencias que le encomienda la legislación sobre seguridad privada; las que le atribuye la legislación en materia de extranjería; el régimen de protección internacional de refugiados, el régimen de apátridas y la protección a desplazados; la administración y régimen de las instituciones penitenciarias; la realización de las actuaciones necesarias para el desarrollo de los procesos electorales; el ejercicio de las competencias sobre protección civil; atención y apoyo a las víctimas del terrorismo y las atribuidas en materia de tráfico, seguridad vial y movilidad sostenible.

Artículo 4. *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 y al sistema de archivos y gestión documental del Departamento.

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 5. *Estructura organizativa de la PSI.*

1. La organización de la seguridad debe tener en cuenta la propia organización del Ministerio del Interior, en consecuencia, las responsabilidades en seguridad de la información deben emerger de todos los ámbitos, garantizándose la actuación coordinada y eficaz.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

2. Sin perjuicio de lo anterior, 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) El Grupo de Trabajo de los Responsables de la Seguridad.
c) Los Grupos de Trabajo para la Seguridad de la Información.
d) El Grupo de Trabajo de los Delegados de Protección de Datos.
e) El Responsable de la Información.
f) El Responsable del Servicio.
g) El Responsable de la Seguridad.
h) El Responsable del Sistema.

Artículo 6. *El Comité Superior para la Seguridad de la Información.*

1. El Comité Superior para la Seguridad de la Información (en adelante, CSSI), se configura como un grupo de trabajo en el seno del Pleno de la Comisión Ministerial de Administración Digital del Departamento, y será el encargado de coordinar todas las actividades relacionadas con la seguridad de los sistemas de información en el ámbito del Ministerio del Interior, ejerciendo 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) Presidencia: La persona titular de la Subsecretaría del Ministerio del Interior.
b) Vicepresidencia: La persona titular de la Secretaría General Técnica.
c) Vocalías: Las personas titulares de los siguientes Centros Directivos:

1.ª Dirección General de la Policía.
2.ª Dirección General de la Guardia Civil.
3.ª Secretaría General de Instituciones Penitenciarias.
4.ª Dirección General de Relaciones Internacionales y Extranjería.
5.ª Dirección General de Política Interior.
6.ª Dirección General de Tráfico.
7.ª Dirección General de Protección Civil y Emergencias.
8.ª Dirección General de Apoyo a Víctimas del Terrorismo.
9.ª Gabinete del Secretario de Estado de Seguridad.

d) Secretaría: con voz y voto, la persona titular de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad de la Secretaría de Estado de Seguridad, 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.
e) Un representante del Grupo de Trabajo de los Delegados de Protección de Datos participará, con voz pero sin voto, en las reuniones del CSSI cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación se hará constar siempre en acta el parecer del Delegado de Protección de Datos.

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

1. El Grupo de Trabajo de Responsables de la Seguridad (en adelante, GTRS), se configura 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.

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) Presidencia: la persona titular de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad

b) Vocalías: las personas responsables de la Seguridad de cada Centro Directivo. Una misma persona puede ser responsable de seguridad de más de un Centro Directivo.

c) Secretaría: Un funcionario de carrera de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad.

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

1. Se constituirá un Grupo de Trabajo para la Seguridad de la Información (en adelante, GTSI) en cada uno de los Centros Directivos del Ministerio del Interior que tenga competencias de gestión de tecnologías de la información y, en particular los siguientes:

a) Grupo de Trabajo para los servicios centrales de la Secretaría de Estado de Seguridad y de la Subsecretaría del Ministerio del Interior

b) Dirección General de la Policía.

c) Dirección General de la Guardia Civil.

d) Secretaría General de Instituciones Penitenciarias.

e) Dirección General de Tráfico.

f) Dirección General de Protección Civil y Emergencias.

g) Entidad de Derecho Público Trabajo Penitenciario y Formación para el Empleo.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

2. Se establece la posibilidad de que, en razón de infraestructuras compartidas, se puedan agrupar algunos de los grupos de trabajo citados en el apartado anterior.

3. Los GTSI ejercerán 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 a la normativa en vigor en materia de seguridad y privacidad.

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.

4. La composición final y funcionamiento de cada GTSI será determinada por el titular del Centro Directivo de entre los funcionarios de carrera 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.

5. 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 su organización, 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.

6. 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.

7. El Delegado de Protección de Datos del Centro Directivo participará, con voz pero sin voto, en las reuniones del GTSI cuando en el mismo vayan a abordarse cuestiones relacionadas con el tratamiento de datos de carácter personal, así como siempre que se requiera su participación. En todo caso, si un asunto se sometiese a votación se hará constar siempre en acta el parecer del Delegado de Protección de Datos.

8. La composición final de cada GTSI se comunicará a la Secretaría del Comité Superior para la Seguridad de la Información para su traslado a la Comisión Ministerial de Administración Digital, en el plazo máximo de un mes desde su constitución.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

Artículo 9. *El Grupo de Trabajo de los Delegados de Protección de Datos.*

1. Se constituye el Grupo de Trabajo de los Delegados de Protección de Datos (GTDPD, en adelante), compuesto por los Delegados de Protección de Datos (DPD en adelante) nombrados en el Ministerio del Interior:

a) DPD de la Dirección General de la Policía.
b) DPD de la Dirección General de la Guardia Civil.
c) DPD de la Secretaría General de Instituciones Penitenciarias.
d) DPD de la Dirección General de Tráfico.
e) DPD de la Secretaría de Estado de Seguridad.
f) DPD del Ministerio, para el ámbito del Ministro, y de la Subsecretaría del Interior (excluida la Dirección General de Tráfico).

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

a) Supervisar la normativa de seguridad del ministerio en relación al cumplimiento de lo dispuesto en el Reglamento general de protección de datos, en otras disposiciones de protección de datos de la Unión Europea o de los Estados miembros en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
b) Normalizar metodologías de acción, criterios comunes y documentación general a utilizar en materia de protección de datos personales.
c) Proponer recomendaciones o sugerencias que considere oportunas relativas a materia de protección de datos a los responsables y encargados de tratamiento del Ministerio del Interior.
d) En las reuniones del GTDPDS podrán participar cuantos asesores, internos o externos, estimen necesarios los miembros del mismo.

Artículo 10. *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 11. *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 citado Real Decreto.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

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.
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 12. *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 con competencias de gestión de tecnologías de comunicación, en particular los señalados en el artículo 10.1 se designará un Responsable de Seguridad entre los funcionarios de carrera 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 de carrera 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.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

Artículo 13. *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.

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.

d) Para las demás funciones que por su naturaleza así lo requieran, se coordinará con la Secretaría General Técnica, especialmente a los efectos de eliminación de la información, de transferencia al archivo electrónico único y de cuantas otras actuaciones estén comprendidas en el marco del Sistema de Archivos del Ministerio del Interior.

Artículo 14. *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 15. *Gestión de riesgos.*

1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad basada en los riesgos y de reevaluación periódica, según los artículos 6 y 9, respectivamente, del Real Decreto 3/2010, de 8 de enero, y de acuerdo con el artículo 24 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, Reglamento general de protección de datos).

En caso de que el análisis de gestión de riesgos de acuerdo con el Reglamento general de protección de datos agraven las medidas a implantar respecto de las previstas en el Real Decreto 3/2010, de 8 de enero, tienen prioridad las medidas de acuerdo con el artículo 24.1 del Reglamento general de protección de datos.

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 16. *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

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

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.
4. El GTSI establecerá los mecanismos necesarios para compartir la documentación derivada del desarrollo normativo con el propósito de normalizarlo, en todo el ámbito de aplicación de la PSI.

Artículo 17. *Protección de datos de carácter personal: la política de privacidad.*

1. En el ámbito del Ministerio del Interior la garantía de la protección de datos de carácter personal de las actividades de tratamiento es un objetivo compartido por todas las unidades del departamento que se rige por los siguientes principios:

a) Licitud, lealtad y transparencia.
b) Limitación de la finalidad.
c) Minimización de datos.
d) Exactitud.
e) Limitación del plazo de conservación.
f) Integridad y confidencialidad.
g) Responsabilidad proactiva.

2. Para su consecución se establecen las siguientes directrices:

a) Estructura organizativa: En el ámbito del Ministerio del Interior se nombran los siguientes Delegados de Protección de Datos (en adelante, DPD) que asumen, en su ámbito de competencias, las funciones recogidas en el artículo 39 del Reglamento general de protección de datos:

1.º DPD de la Dirección General de la Policía.
2.º DPD de la Dirección General de la Guardia Civil.
3.º DPD de la Dirección General de Tráfico.
4.º DPD de la secretaría General de Instituciones Penitenciarias.
5.º DPD de la Secretaría de Estado de Seguridad.
6.º DPD del Ministerio, que actúa como coordinador, al que corresponden el resto de ámbitos del Ministerio.

La actuación de los DPD se regirá por el principio de independencia, por lo que no recibirán ninguna instrucción en lo que respecta al desempeño de sus funciones. Podrán

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

estar asistidos por grupos de trabajo integrados por representantes de las unidades administrativas de su ámbito de actuación.

b) Actividades de tratamiento: Se entiende por tratamiento cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

De acuerdo con el Reglamento general de protección de datos, y en especial con lo dispuesto en su artículo 17, el responsable del tratamiento es el titular de la Unidad Administrativa que determine los fines y medios del tratamiento; con carácter general, se corresponde con el titular de la unidad en que se produzca la operación sobre los datos; en los casos en que no se corresponda la definición legal del responsable del tratamiento con el titular de la unidad en que se produzca la operación sobre los datos o haya varias unidades en las que se produzca la operación de los datos, el titular del centro directivo determinará el responsable del tratamiento, para lo cual puede ser asesorado por parte del DPD.

Para todos aquellos tratamientos de datos que procesen datos de carácter personal que se realicen en el Ministerio del Interior, los responsables de tratamiento deberán proporcionar la información necesaria para elaborar un Registro con sus Actividades de Tratamiento. Los DPD darán instrucciones sobre la herramienta y el apoyo necesario para el mantenimiento del citado registro, cuyo contenido deberá corresponderse con la establecida en el artículo 30 del Reglamento general de protección de datos, incluyendo también su base legal.

c) Cláusulas informativas: Para garantizar la adecuación permanente de las cláusulas informativas en materia de privacidad, os responsables de tratamiento deberán verificar el cumplimiento continuo de la inclusión de cláusulas informativas sobre el tratamiento de datos personales (artículos 13 y 14 del Reglamento general de protección de datos), en especial en el momento previo a la recogida de datos personales, tanto en formularios en papel como en medios electrónicos.

d) Procedimientos de relación entre las agencias de control, DPD, responsables de tratamiento y ciudadanos: Los ciudadanos pueden ejercitar sus derechos directamente a los responsables de tratamiento, o bien hacerlo a un DPD o incluso directamente ante una agencia de control como, por ejemplo, la Agencia Española de Protección de Datos. Los responsables de tratamiento responderán a las peticiones, pudiendo actuar el DPD correspondiente como intermediario con el ciudadano y con otras administraciones, así como llevando la interlocución con las agencias de control.

e) Gestión de riesgos de privacidad: La gestión de riesgos de privacidad se alineará con el análisis de riesgos de la seguridad. Los DPD podrán, a petición del responsable del tratamiento, proporcionar asesoramiento y herramientas específicas tanto para esta gestión de riesgos, como para la realización de evaluaciones de impacto en la privacidad para los tratamientos, en especial los de alto riesgo.

f) Revisión jurídica de los contratos, acuerdos y convenios con encargados de tratamiento: Los DPD proporcionarán modelos de cláusulas tipo y asesoramiento para la adecuación de contratos, acuerdos y convenios que incluyan el tratamiento de datos personales.

g) Procedimiento de comunicación de brechas de seguridad: Los DPD definirán los protocolos correspondientes, coordinados con los responsables de seguridad, para la comunicación de brechas de seguridad que afecten a información con datos de carácter personal.

h) Procedimiento de privacidad desde el diseño: Los DPD definirán y difundirán un procedimiento de privacidad desde el diseño que tendrá por objetivo el introducir un protocolo dentro del ciclo de vida del desarrollo y mantenimiento de sistemas de información que garantice que se tienen en cuenta las exigencias de seguridad derivadas del manejo de datos personales.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

i) Auditorías de privacidad y revisión continua de las medidas de privacidad: Los DPD fomentarán procesos de auditoría periódica encaminados a la mejora continua del cumplimiento normativo en materia de protección de datos y a la implantación de las medidas correctoras necesarias para mejorar la seguridad de los datos personales.

j) Actuaciones de formación y concienciación: Los DPD realizarán una planificación de actuaciones periódicas de formación y concienciación al personal en materia de privacidad. Asimismo, se impulsará la formación en materia de gestión documental y archivo.

3. 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 la normativa de protección de datos en vigor que afecte al sistema de información concreto.

Artículo 18. *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 19. *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.

CAPÍTULO II

Directrices de seguridad de la información para la difusión de resultados provisionales en materia de procesos electorales

Artículo 20. *Ámbito de aplicación.*

1. Las presentes directrices se aplican a todos los servicios y sistemas TIC que participen de manera activa o pasiva en el proceso de Difusión de Resultados Provisionales en Procesos Electorales.

2. Se incluye a todo el personal, sistemas informáticos, recursos, infraestructura, proveedores y terceros que la Subsecretaría del Interior emplea para la ejecución del proceso de Difusión de Resultados Provisionales en Procesos Electorales.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

Todo el personal interno o externo deberá conocerlas y aplicarlas como parte de las tareas propias de su función dentro del organismo.

3. Queda excluido de las presentes directrices todo aquel proceso electoral que no sea gestionado por el Ministerio del Interior o cualquier otro del que no forme parte.

Artículo 21. *Objetivo.*

1. Los sistemas de información que integran el proceso de Difusión de Resultados Provisionales en Procesos Electorales requieren unos niveles elevados de confidencialidad, disponibilidad e integridad debido principalmente, al grado de criticidad de la información y la grave repercusión e impacto que se produciría en la ciudadanía, en caso de afectación negativa.

Por ello, atendiendo a los objetivos de seguridad del departamento, requieren de unas medidas de seguridad adecuadas, que en términos de capacidad de gestión, confidencialidad, integridad, disponibilidad de la información y mejora continua permitan desarrollar su función con plena garantía y eficacia.

2. Estas directrices se sustentarán en la creación, implantación, revisión y mejora continua de un Sistema de Gestión de la Seguridad de la Información, fundamentado en los procesos de análisis y gestión de riesgos.

Dicho Sistema de Gestión de Seguridad de la Información se traducirá en un marco normativo interno de aplicación, estructurando toda la información en documentación (Políticas, Normativa, Procedimientos, Manuales, Instrucciones Técnicas, entre otras), que determinará el modo de asegurar los distintos activos y procesos que conforman la Difusión de Resultados Provisionales en Procesos Electorales.

Artículo 22. *Subcomité de Seguridad de la Información para la Difusión de Resultados Provisionales en Procesos electorales.*

1. El Subcomité de Seguridad de la Información para la Difusión Provisional en Procesos Electorales, adscrito al comité Superior para la Seguridad de la Información del Ministerio del Interior, cuyo ámbito de actuación es la seguridad de la información en procesos electorales.

2. El Subcomité está compuesto por los siguientes miembros:

a) Presidencia: La persona titular de la Subsecretaría del Ministerio del Interior.

b) Vicepresidencia: La persona titular de la Dirección General de Política Interior.

c) Secretaría: La persona titular de la Subdirección General de Política Interior y Procesos Electorales.

d) Vocalías:

1.º La persona titular de la Subdirección General de Sistemas de Información y Comunicaciones por su condición de Responsable de Seguridad de la Información del Grupo de Trabajo para los Servicios Centrales de la Secretaría de Estado de Seguridad y de la Subsecretaría del Ministerio del Interior, y Presidente del Grupo de Trabajo de Responsables de la Seguridad.

2.º La persona titular de la Subdirección General de Calidad de los Servicios e Innovación por su condición de Delegado de Protección de Datos del Ministerio del Interior, y Presidente del Grupo de Trabajo de los Delegados de Protección de Datos, con voz pero sin voto.

3.º Un funcionario de carrera del subgrupo A1 de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, designado por su titular.

3. Son funciones del Subcomité, en el ámbito de los procesos electorales:

a) Aprobar las normas específicas de seguridad de la información y normas de seguridad TIC.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

b) Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.

c) Coordinar los planes de continuidad del servicio entre las diferentes áreas para asegurar una actuación sin fisuras en caso de que deban ser activados.

d) Coordinar y aprobar las propuestas recibidas en materia de seguridad de los diferentes órganos y unidades del Ministerio.

e) Recabar del Responsable de Seguridad de la Información informes regulares del estado de la seguridad del servicio y de los posibles incidentes.

f) Aprobar la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a la segregación de funciones.

g) Establecer y aprobar la metodología y criterios para el análisis de riesgos.

h) Proponer para su aprobación, cualquier modificación de las Directrices de Seguridad de la Información en materia de procesos electorales.

4. El Subcomité de Seguridad de la Información para la Difusión de Resultados Provisionales en Procesos Electorales se reunirá con la periodicidad que determine su Presidencia.

Artículo 23. *Responsable de la información.*

1. El Responsable de la Información tendrá la potestad de establecer los requisitos de la información en materia de seguridad determinando así el nivel de seguridad asociado a los mismos en cada dimensión. En concreto, establecerá los requisitos de integridad, confidencialidad, disponibilidad y aquellos otros que considere oportunos. Dada la criticidad que conlleva este papel, corresponde a la persona titular de la Dirección General de Política Interior ejercer dicha responsabilidad.

2. El responsable de la información podrá ser asistido por las personas o unidades del Ministerio que estime necesario, además de, en su caso, por otros organismos con competencias en el ámbito de la seguridad de la información

3. 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, de acuerdo con los informes que reciba del Responsable de Seguridad de la Información.

b) Con el apoyo del Responsable del Servicio de Procesos Electorales, velar por la realización de los preceptivos análisis de riesgos, seleccionando las salvaguardas que se han de implantar, a propuesta del Responsable de Seguridad de la Información.

c) Aceptar los riesgos residuales a los que se expone la información, una vez realizado el análisis de riesgos e implantadas la salvaguardas que hayan sido seleccionadas.

Artículo 24. *Responsable del Servicio de Procesos Electorales.*

1. El Responsable del Servicio de Procesos Electorales tendrá la potestad de establecer los requisitos del servicio en materia de seguridad determinando así el nivel de seguridad asociado a los mismos en cada dimensión analizada para la protección de la información. En concreto, establecerá los requisitos de disponibilidad, y aquellos otros que considere oportuno: confidencialidad, integridad, accesibilidad, interoperabilidad, etc. Dada la relevancia que existe en establecer los requisitos de seguridad en el servicio, corresponde a la persona titular de la Subdirección General de Política Interior y Procesos Electorales, ejercer el presente papel como órgano dependiente de la Dirección General de Política Interior del Ministerio del Interior.

2. El responsable del servicio podrá ser asistido por las personas o unidades del Ministerio que estime conveniente el Responsable de la Información además de, en su caso, por otros organismos con competencias en el ámbito de la seguridad de la información.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

3. Serán funciones del Responsable del Servicio de Procesos Electorales, 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 en todas sus dimensiones, de acuerdo con los informes que reciba del Responsable de Seguridad de la Información.
b) Junto al Responsable de la Información, velar por la realización de los preceptivos análisis de riesgos, seleccionando las salvaguardas que se han de implantar, a propuesta del Responsable de Seguridad de la Información.
c) Aceptar los riesgos residuales a los que se expone los servicios, una vez realizado el análisis de riesgos e implantadas las salvaguardas que hayan sido seleccionadas.

Artículo 25. *Responsable del Sistema en Procesos Electorales.*

1. El Responsable de los Sistemas en Procesos Electorales tendrá la responsabilidad de desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de velar por que se cumplan las especificaciones que se dicten, garantizar su instalación y de verificar su correcto funcionamiento. Corresponde a la persona titular de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad desempeñar el papel de Responsable del Sistema en Procesos Electorales.
2. El Responsable de los Sistemas en Procesos Electorales podrá ser asistido por las personas o unidades del Ministerio que estime conveniente el Responsable de la Información además de, en su caso, por otros organismos con competencias en el ámbito de la seguridad de la información.
3. Son funciones del Responsable de los Sistemas en Procesos Electorales:

a) Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
b) Asegurar que las medidas específicas de seguridad se integren adecuadamente.
c) Proponer, en su caso, la suspensión total o parcial de la prestación del Servicio, si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión deberá ser informada, consensuada y aprobada, con carácter previo, en el Subcomité de Seguridad de la Información en Procesos Electorales

Artículo 26. *Responsable de Seguridad de la Información.*

1. El Responsable de Seguridad de la Información deberá satisfacer los requisitos de seguridad de la información y de los servicios que hayan sido analizados y establecidos respectivamente por sus responsables. Corresponderá al titular de la jefatura del área responsable de la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad (SGSICS) desempeñar este papel.
2. Serán funciones del Responsable de la Seguridad de la Información, dentro de su ámbito de actuación, las siguientes:

a) Elaborar la normativa específica de seguridad que desarrolla la presente Política de Seguridad de la Información.
b) Aprobar los procedimientos operativos de seguridad.
c) Mantener la seguridad de la información manejada y de los servicios digitales prestados por los sistemas de información.
d) Realizar o promover las auditorías preceptivas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información.
e) Realizar el seguimiento y control del estado de seguridad del sistema de información.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

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

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

h) Elaborar planes de concienciación y formación.

i) Supervisar el registro de activos.

El Responsable de Seguridad de la Información recabará las respuestas y soluciones a las cuestiones que le sean planteadas en el Comité de Seguridad de la Información.

Artículo 27. *Gestión de riesgos.*

Todos los sistemas sujetos a estas directrices serán incluidos en los correspondientes análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Estos análisis se llevarán a cabo periódicamente y, en todo caso, se repetirán:

a) En cada proceso electoral.

b) Cuando cambie la información manejada.

c) Cuando se modifiquen los servicios prestados.

d) Cuando ocurra un incidente grave de seguridad que afecte al ámbito de la seguridad de la información.

e) Cuando se informen vulnerabilidades graves que afecten al ámbito de la seguridad de la información.

Para la realización de los análisis de riesgos, el Subcomité de Seguridad de la Información en procesos electorales establecerá un valor de referencia para los diferentes tipos de información manejados y servicios prestados, acorde a la normativa aplicable.

Artículo 28. *Deberes y responsabilidades y protección de datos.*

Lo previsto en la Política de Seguridad de la Información de la Información en el ámbito de la Administración electrónica del Ministerio del Interior se aplicará a las presentes Directrices.

Artículo 29. *Auditoría.*

Se realizarán las correspondientes auditorías en cada uno de los procesos electorales en las que forme parte el Ministerio del Interior, tanto para validar los cambios que se hayan realizado como para verificar el grado de cumplimiento de la misma, siendo éstas las siguientes:

a) Auditorías previas: estas auditorías deberán estar finalizadas 15 días antes de la jornada electoral. Se considerarán finalizadas y conformes, cuando se hayan aplicado todas las medidas que por parte del Comité de Seguridad de la Información –al que se refiere el apartado 4.1– se consideren necesarias.

b) Auditoría de Evaluación Continua: Con el fin de actualizar la Política de Seguridad de la Información en cada proceso electoral, durante los 30 días posteriores al día de las votaciones, se iniciará una auditoría con la finalidad de identificar aquellos objetivos de seguridad cumplidos y los puntos de mejora que se hayan detectado, para su aplicación en futuros procesos, previa revisión, en su caso, por parte del citado Comité de Seguridad de la Información.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es

Artículo 30. *Revisión.*

Corresponde al Subcomité de Seguridad de la Información para la Difusión Provisional en Procesos Electorales la revisión y actualización de las presentes Directrices Generales.

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

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

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la 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.

Disposición final primera. *Publicidad.*

La presente orden se publicará, además de en el «Boletín Oficial del Estado», en la sede electrónica del Ministerio del Interior y sus sedes asociadas.

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, 10 de abril de 2019.–El Ministro del Interior, Fernando Grande-Marlaska Gómez.

cve: BOE-A-2019-5536
Verificable en http://www.boe.es