III. OTRAS DISPOSICIONES

MINISTERIO DE FOMENTO

3482 *Resolución de 1 de diciembre de 2014, de Puertos del Estado, por la que se publica la de 6 de noviembre de 2014, por la que se aprueba la Política de Seguridad de la Información.*

Con fecha 6 de noviembre de 2014, esta Presidencia resolvió aprobar la Política de Seguridad de la Información de Puertos del Estado.

En su virtud, se dispone la publicación, en el «Boletín Oficial del Estado», de la referida resolución, que se adjunta como Anexo a la presente resolución.

Madrid, 1 de diciembre de 2014.–El Presidente de Puertos del Estado, José Llorca Ortega.

ANEXO

Resolución por la que se aprueba la Política de Seguridad de la Información de Puertos del Estado.

De conformidad con lo previsto 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, y de conformidad con las atribuciones conferidas en el artículo 22.2.d) del Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 2/2011, de 5 de septiembre, acuerdo aprobar la Política de Seguridad de la Información de Puertos del Estado, en los términos recogidos en el documento anexo a la presente resolución.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

(Octubre 2014)

Índice

cve: BOE-A-2015-3482

CAPÍTULO I

Política de Seguridad de la Información de Puertos del Estado

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, señala entre sus fines la creación de unas condiciones de confianza en el uso de los medios electrónicos, estableciéndose para ello 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 garantizando la seguridad de los sistemas, los datos las comunicaciones y los servicios electrónicos, fines que han sido desarrollados por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica. Asimismo, la información tratada en los sistemas electrónicos a los que se refiere el ENS estará protegida teniendo en cuenta los criterios establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

El ENS, por su parte, establece el marco regulatorio de la Política de Seguridad de la Información, que se plasma en un documento, accesible y comprensible para todos los miembros, 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 crítico. La Política de Seguridad debe ser conforme con los requisitos que figuran en el ENS que establece que todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de una Política de Seguridad de la Información aprobada por el órgano superior competente.

En virtud de lo expuesto, la Política de Seguridad de la Información de Puertos del Estado se regirá por las siguientes normas:

Artículo 1. *Objeto y ámbito de aplicación.*

1. Constituye el objeto de la presente Resolución la aprobación de la Política de Seguridad de la Información, en adelante Política de Seguridad, del Organismo Público Puertos del Estado, y el establecimiento de un marco organizativo y tecnológico de la misma.

cve: BOE-A-2015-3482

2. Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos y materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

3. Debe ser conocida y cumplida por todo el personal de Puertos del Estado, independientemente del puesto, cargo y responsabilidad dentro del mismo.

Artículo 2. *Misión.*

Corresponden a Puertos del Estado las competencias y funciones establecidas en los artículos 17 y 18 del Real Decreto Legislativo 2/2011, de 5 de septiembre, por el que se aprueba el Texto Refundido de la Ley de Puertos del Estado y la Marina Mercante.

Artículo 3. *Legislación y normativa de referencia.*

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

– Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

– 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.

– 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.

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

– 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, de protección de datos de carácter personal.

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

– Ley 59/2003, de 19 de diciembre, de firma electrónica.

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

Artículo 4. *Principios de la Seguridad de la Información.*

Los principios que conforman la Política de Seguridad de la Información son los siguientes:

– La información que posee y trata Puertos del Estado tiene un valor muy importante para el propio organismo así como para los ciudadanos, por lo que es primordial protegerla.

– La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra.

– La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.

– La Seguridad de la Información es responsabilidad de todos. Todas las personas que tiene acceso a la información de Puertos del Estado deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas.

– La Seguridad de la Información no es algo estático, debe ser constantemente controlada y periódicamente revisada.

– La información relativa a las personas y ciudadanos que trate Puertos del Estado pertenece a ellos y no a la Administración conforme a la normativa en protección de datos de carácter personal.

– Todos aquellos activos (infraestructura, soportes, sistemas, comunicaciones, etc.) donde reside la información, viaja o es procesada, deben estar adecuadamente protegidos.

cve: BOE-A-2015-3482

– Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirá como mínimo las medidas de seguridad impuestas por el Esquema Nacional de Seguridad, así como las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.

– El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importantes la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

CAPÍTULO II

Organización de la Seguridad de la Información

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

1. Para la gestión de la Seguridad de la Información, se crea el Comité de Gestión de la Seguridad de la Información, en adelante el Comité de Seguridad, dentro del ámbito de la presente Política de Seguridad formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en Puertos del Estado y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos de carácter personal y seguridad. Es el encargado de impulsar la implementación de la presente Política de Seguridad.

2. El Comité de Seguridad estará compuesto por los siguientes miembros:

a) Presidente: Rolando Lago Cuervo.
b) Secretaría: Gabriel Argüelles Pintos.
c) Vocalía: Sebastián Espinar Cerrejón.
d) Vocalía: Celia Tamarit de Castro.
e) Vocalía: Jaime Luezas Alvarado.
f) Vocalía: Álvaro Sánchez Manzanares.

3. El Comité de Seguridad, se reunirá con carácter ordinario, al menos una vez cada tres meses, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

4. El Secretario del Comité de Seguridad levantará actas de sus reuniones.

5. A las sesiones del Comité de Seguridad podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su Presidente.

6. Son funciones del Comité de Seguridad las siguientes:

a) Identificar los objetivos de Puertos del Estado en el ámbito de la Seguridad de la Información.

b) Elaborar la Política de Seguridad, establecer los criterios de revisión de la misma, revisarla, distribuirla y velar por su cumplimiento.

c) Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en Puertos del Estado.

d) Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnico y de control, los sistemas y servicios de Puertos del Estado.

e) Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.

f) Aprobar los nombramientos de responsables y responsabilidades en materia de seguridad de la información.

g) Valorar el grado de conformidad de los procedimientos implantados en Puertos del Estado con las normas definidas en la política, estableciendo planes de mejora para aquellos que requieran de una modificación para su conformidad.

cve: BOE-A-2015-3482

h) Supervisar las normativas y procedimientos de seguridad que se definan para dar cumplimiento y desarrollo a la Política de Seguridad.

i) Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.

j) Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la Política de Seguridad.

k) Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de las Administraciones en materia de Seguridad.

l) Promover la formación y concienciación en materia de Seguridad de la Información a todo el personal.

m) Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la Seguridad de la Información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener la seguridad de los sistemas de Puertos del Estado.

n) Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en Puertos del Estado.

CAPÍTULO III

Roles, funciones y responsabilidades en Materia de seguridad

Artículo 6. *Responsables de la Información.*

1. Responsables de clasificar la información conforme a los criterios y categorías establecidas en el ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad), dentro del marco establecido en el Anexo I del ENS.

2. Son los encargados, junto a los Responsables de los Servicios y contando con la participación y asesoramiento del Responsable de Seguridad y del Responsable del Sistema de Información, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

3. Son los responsables, junto con los Responsables de los Servicios, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

4. 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 gestiones.

5. En caso de que los Responsables de la Información no puedan ser nominados en personas será asignado al Comité de Seguridad.

Artículo 7. *Responsables de los Servicios.*

1. Responsables de determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad).

2. Esta responsabilidad recaerá en el titular del órgano que gestione cada servicio.

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

4. Son los responsables, junto con los Responsables de la Información, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

5. En caso de que los Responsables de los Servicios no puedan ser nominados en personas será asignado al Comité de Seguridad.

cve: BOE-A-2015-3482

Artículo 8. *Responsable de Seguridad de la Información.*

1. Responsable de que los servicios y sistemas de información de Puertos del Estado se mantengan con el mayor grado de seguridad atendiendo a los principios de:

a) Confidencialidad: la información asociada a los servicios electrónicos al ciudadano solo debe poder ser conocida por las personas autorizadas para ello.
b) Integridad: la información asociada a los servicios electrónicos al ciudadano no debe ser alterada por personas no autorizadas.
c) Disponibilidad: garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma siempre que lo requieran, así como garantía de que los servicios relativos a la Administración Electrónica permanecerán disponibles.

2. Son funciones del Responsable de Seguridad:

a) Supervisar el cumplimiento de la presente Política, de sus normas y procedimientos derivados.
b) Asesorar en materia de seguridad a los integrantes de Puertos del Estado que así lo requieran.
c) Coordinar la interacción con otros organismos especializados.
d) Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
e) Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS.
f) Asesorar, en colaboración con los Responsables de los Sistemas, los Responsables de los Servicios y de la Información, en la realización del análisis y gestión de riesgos, elevando el informe resultante al Comité de Seguridad.
g) Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
h) Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.

3. Respecto a la documentación, son funciones del Responsable de Seguridad:

a) Aprobar y proponer al Comité de Seguridad la documentación de seguridad de segundo nivel (Normativas y Procedimientos de Seguridad) de obligado cumplimiento.
b) Supervisar la documentación de tercer nivel (Procedimientos Técnicos de Seguridad) de obligado cumplimiento.
c) Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.

4. En aquellos sistemas de información que por su complejidad, distribución, separación física de elementos o números de usuarios se necesitara de personal adicional para llevar a cabo las funciones del Responsable de Seguridad, el Responsable de Seguridad podrá designar cuantos Responsables de Seguridad Delegados considere necesarios, incluyendo los Responsables de Seguridad relativos a la LOPD. Los Responsables de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de Seguridad teniendo dependencias funcionales directas con él.
5. El Responsable de Seguridad será nombrado y cesado por el Comité de Seguridad.

cve: BOE-A-2015-3482

Artículo 9. *Responsables de los Sistemas de Información.*

1. Personal designado cuyas responsabilidades son:

a) Desarrollo, operación y mantenimiento del sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
b) Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.
c) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
d) Elaborar procedimientos técnicos de seguridad de los sistemas de información.
e) Elaborar planes de continuidad de los sistemas de información.

2. Podrá acordar la suspensión del manejo de determinada 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 deberá ser acordada con los Responsables de la Información afectada, los Responsables del Servicio y el Responsable de Seguridad antes de ser ejecutada.
3. En aquellos sistemas que por su complejidad, distribución, separación física de elementos o número de usuarios se necesite personal adicional para llevar a cabo las funciones de Responsable de Sistemas, se podrán designar cuantos Responsables de Sistemas Delegados se consideren oportunos. La designación y delegación de funciones en los Responsables de Sistemas Delegados corresponde al Responsable del Sistema, sin perjuicio de que la responsabilidad final siga recayendo sobre el Responsable del Sistema. Los Responsables de Sistemas Delegados se harán cargo en su ámbito de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de Información correspondiente, y tendrá dependencia funcional directa del Responsable del Sistema que es a quién reporta.

Artículo 10. *Administradores de la Seguridad de los Sistemas de Información.*

1. Personal designado, dependiente del Responsable de Seguridad de la Información, cuyas funciones son las siguientes:

a) Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información.
b) Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
c) Gestionar las autorizaciones concedidas a los usuarios del sistema, en particular, los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
d) Aplicar la documentación de tercer nivel.
e) Aprobar los cambios en la configuración vigente del sistema de información.
f) Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
g) Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
h) Informar al Responsable de Seguridad de la Información y a los Responsables de los Sistemas afectados de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
i) Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

cve: BOE-A-2015-3482

2. En caso de que determinados Sistemas de Información que por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite personal adicional para llevar a cabo las funciones de Administrador de la Seguridad del Sistema, se podrán designar Administradores de Seguridad del Sistema Delegados.

3. Los Administradores de Seguridad de los Sistemas serán propuestos por el Responsable de Seguridad de la Información.

Artículo 11. *Resolución de conflictos.*

1. 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 Responsable de Seguridad.

Artículo 12. *Obligaciones del Personal.*

1. Todo el personal de Puertos del Estado, así como el que preste servicios al Organismo relacionados con los sistemas de información, tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas y procedimientos derivados de la misma, tales como las relativas a la protección de datos de carácter personal, siendo responsabilidad del Comité de Seguridad disponer de los mecanismos necesarios para que la información llegue a todos.

2. El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta podrá acarrear el inicio de medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

CAPÍTULO IV

Asesoramiento especializado en materia de seguridad

Artículo 13. *Asesoramiento especializado.*

1. El Responsable de Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en Puertos del Estado con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

Artículo 14. *Cooperación entre organismos y otras Administraciones Públicas.*

1. A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, Puertos del Estado mantendrá contactos periódicos con organismos y entidades especializadas en temas de seguridad.

Artículo 15. *Revisión independiente de la Seguridad de la Información.*

1. El Comité de Seguridad propondrá la realización de revisiones periódicas independientes sobre la vigencia e implementación de la Política de Seguridad con el fin de garantizar que las prácticas en Puertos del Estado reflejan adecuadamente sus disposiciones.

CAPÍTULO V

Protección de datos, formación y gestión

Artículo 16. *Tratamiento de los datos de carácter personal.*

1. Para el tratamiento de datos de carácter personal en los sistema de información se seguirá en todo momento lo desarrollado en el documento de seguridad y su documentación asociada conforme a lo exigido en el Título VIII de las medidas de

cve: BOE-A-2015-3482

seguridad en el tratamiento de datos de carácter personal del 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, de Protección de Datos de Carácter Personal.

Artículo 17. *Formación y concienciación.*

1. El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal de Puertos del Estado y a todas las actividades de acuerdo al principio de seguridad integral recogido en el artículo 5 del ENS. A estos efectos, Puertos del Estado, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.
2. El Comité de Seguridad aprobará una Política de formación y concienciación en el tratamiento seguro de la información con los siguientes objetivos:

a) Formación sobre la protección de la información de datos de carácter personal, orientada a los responsables de los ficheros y hacia los usuarios con privilegios sobre los datos.
b) Formación sobre los procedimientos desarrollados.

Artículo 18. *Análisis y gestión de riesgos de los sistemas de información.*

1. Puertos del Estado asume el compromiso de controlar los riesgos de seguridad, así como dar cumplimiento a la legislación y normas internas vigentes bajo un proceso de mejora continua conforme a los marcos y metodologías existentes en la actualidad en análisis y gestión de riesgos.
2. Con el objetivo de conocer el nivel de exposición de los activos de información a los riesgo y amenazas en seguridad, los Responsables de Sistemas de Información realizarán, con periodicidad al menos anual, un análisis de riesgos cuyas conclusiones se plasmarán en actuaciones para tratar y mitigar el riesgo, e incluso replantear la seguridad de los sistemas en caso necesario.
3. Se realizará un análisis de riesgos de los sistemas de información en periodos inferiores a un año cuando:

a) Se modifique la información manejada.
b) Se modifiquen los servicios prestados.
c) Ocurran incidentes graves de seguridad.
d) Se reporten vulnerabilidades graves.

4. Las conclusiones de los análisis de riesgos serán elevadas al Responsable de Seguridad y éste al Comité de Seguridad.

CAPÍTULO VI

Estructura normativa

Artículo 19. *Estructura de la documentación de seguridad.*

1. La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

a) Primer nivel: Política de Seguridad de la Información.
b) Segundo nivel: Normativas y Procedimientos de Seguridad.
c) Tercer nivel: Procedimientos Técnicos de Seguridad.
d) Cuarto nivel: Informes, registros y evidencias electrónicas.

cve: BOE-A-2015-3482

Artículo 20. *Primer nivel: Política de Seguridad.*

1. Documento de obligado cumplimiento por todo el personal, interno y externo, de Puertos del Estado, recogido en el presente documento y aprobada mediante Resolución de la Presidencia de Puertos del Estado.

Artículo 21. *Segundo Nivel: Normativas y Procedimientos de Seguridad.*

2. De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente.
3. La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Responsable de Seguridad bajo la supervisión del Comité de Seguridad.

Artículo 22. *Tercer Nivel: Procedimientos Técnicos de Seguridad.*

1. Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.
2. La responsabilidad de aprobación de estos procedimientos técnicos es del Responsable del Sistema de Información correspondiente, bajo la supervisión del Responsable de Seguridad. En caso de que los procedimientos afectaran a varios sistemas de información será responsabilidad del Responsable de Seguridad el aprobarlos.

Artículo 23. *Cuarto Nivel: Informes, registros y evidencias electrónicas.*

1. Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.
2. La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información en su ámbito.

Artículo 24. *Otra documentación.*

1. Se podrá seguir en todo momento los procedimientos STIC, las normas STIC, las instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400, 500 y 600.

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

La aplicación de esta orden/resolución no conllevará incremento de gasto público, atendiéndose el funcionamiento del Comité de Seguridad y el resto de Responsables mencionados en el presente documento con los recursos humanos y materiales de que dispone Puertos del Estado.

Disposición final primera. *Publicidad de la Política de Seguridad.*

La presente Resolución se publicará, además de en el «Boletín Oficial del Estado», en la sede electrónica de Puertos del Estado.

Disposición final segunda. *Entrada en vigor.*

La Política de Seguridad que se aprueba en esta Resolución será aplicable a partir del día siguiente al de su publicación en el «Boletín Oficial del Estado».

cve: BOE-A-2015-3482