Puerto de Cartagena

Autoridad Portuaria de Cartagena

Política de Seguridad de la Información

Marco normativo de seguridad de la información

Versión 3.0
Fecha de aprobación: 25/02/2020

Índice

Control sobre la documentación.

DOCUMENTO / ARCHIVO			
Titulo		Detalle/Asunto	Plan
Archivo	ENT-001-Política de Seguridad de la Información de la APC v3.0.pdf	Soporte lógico	Documento

CONTROL DEL DOCUMENTO			
Preparado por	Revisado por	Aprobado por	Autorizado por
JASR	CSI	CSI	CSI

REGISTRO DE CAMBIOS				
Versión	Páginas	Fecha	Descripción del cambio	Editor
2.1	22	05/2020	Borrador Documento inicial	Telefónica
3.0	22	25/02/2021	Nueva Política de Seguridad de la Información. Cambios Legales, Miembros y Roles	JASR

1 Introducción

La Autoridad Portuaria de Cartagena, (en adelante la APC), depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Por este motivo la información constituye un activo crucial para la prestación de los servicios portuarios. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

El Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de enero), en su artículo 11 establece que "*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*".

Asimismo, la información tratada en los sistemas electrónicos a los que se refiere el ENS estará protegida teniendo en cuenta los criterios establecidos en el Reglamento Europeo de Protección de Datos 2016/679 que entró en aplicación el 25 de Mayo de 2018 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. 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 críticos.

El Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información tiene por objeto desarrollar el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad.

Este real decreto se aplica a la prestación de los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

De conformidad con lo previsto en el apartado 1 del artículo 6 del Real Decreto-ley 12/2018, la identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y su normativa de desarrollo, en particular el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

La Autoridad Portuaria de Cartagena ha sido designada **Operador de Servicio Esencial** de acuerdo con dicho Real Decreto, **siendo el Centro Criptológico Nacional (CCN-CERT) el CSIRT Nacional de referencia.**

Todos los departamentos deben aplicar las medidas mínimas de seguridad exigidas por la legislación vigente que aplica a la APC (Administración electrónica, Protección de datos de carácter personal, Infraestructuras críticas) así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

El presente texto constituye el Documento de Política de Seguridad de los Sistemas de Información de la Autoridad Portuaria y en él se recoge el conjunto estrategias, medidas tanto técnicas como organizativas, que son necesarias para conseguir un nivel de protección adecuado y permite estar preparados para prevenir, detectar, reaccionar y recuperarse frente incidentes.

La Dirección de la APC entiende su deber de garantizar la seguridad de la información como elemento esencial para el correcto desempeño de sus servicios y, por tanto, soporta los objetivos y principios establecidos en esta política.

2 Alcance

Esta política se aplica a todos los sistemas TIC de la APC y a todos los miembros de la organización, sin excepciones, debiendo ser conocida y cumplida por todo el personal de la APC, independientemente del puesto, cargo y responsabilidad dentro del mismo.

3 Misión

La Autoridad Portuaria de Cartagena tiene entre sus objetivos principales la prestación de los servicios portuarios generales y la autorización y control de los servicios portuarios. De forma estrechamente relacionada con el cumplimiento de esta misión, la APC desea manifestar la necesidad de una infraestructura TIC que garantice la confianza en la tecnología, enfocada a la funcionalidad, conectividad y servicio a los principales actores de la actividad portuaria y el ciudadano como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales.

4 Principios de protección

La presente política de seguridad de la información se basa en unos principios básicos de protección que forman los pilares sobre los que se sustentan y sustentarán todas las actuaciones en materia de seguridad que realice la APC. Estos principios son:

4.1 Prevención, reacción y recuperación

La estrategia en materia de seguridad de la Autoridad Portuaria estará basada en la prevención, detección y corrección de amenazas, para conseguir que éstas no se materialicen o no afecten gravemente a los datos que manejan los sistemas de información o los servicios que se prestan.

Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, estrategias de disuasión y de reducción de la exposición a ciertas amenazas. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen en la mayor brevedad de tiempo que sea posible. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

Todas las medidas de seguridad que se implanten atenderán al menos los requisitos mínimos impuestos por el Esquema Nacional de Seguridad, RGPD, así

como las guías CCN-STIC elaboradas por el Centro Criptológico Nacional del Centro Nacional de Inteligencia.

4.2 Gestión del riesgo

Las decisiones en materia de seguridad deben basarse en el análisis y gestión de riesgos como proceso esencial de seguridad y deberá mantenerse permanentemente actualizado.

La evaluación de riesgos identifica las amenazas y vulnerabilidades y debe ser suficientemente amplia para abarcar los principales factores internos y externos, como factores tecnológicos, físicos y humanos, políticos y servicios de terceros con implicaciones de seguridad.

La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad. Debido a la creciente interconexión de los sistemas de información, la evaluación de riesgos debe incluir la consideración de los posibles daños que pueden proceder de otros o ser causados por terceras personas.

Se realizará un análisis de riesgos de los sistemas de información en periodos inferiores a un año cuando se produzcan cambios relevantes en los sistemas de información o se detecten vulnerabilidades o incidentes que impliquen una necesaria revisión de las medidas adoptadas. Las conclusiones de los análisis de riesgos serán elevadas al Responsable de Seguridad y éste al Comité de Seguridad.

4.3 Seguridad por defecto y en el diseño de las TIC.

Los sistemas de información deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. Un aspecto importante, pero no exclusivo, de este esfuerzo es el diseño y adopción de garantías adecuadas y soluciones para evitar o limitar el daño potencial de amenazas y vulnerabilidades identificadas cuando los sistemas todavía no están funcionando en los entornos reales. La Seguridad debe ser un elemento fundamental de todos los servicios, sistemas y redes de la APC, y una parte integrante del diseño de los sistemas de información y su arquitectura. En los entornos de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

4.4 Gestión de la seguridad y mejora continua.

La gestión de la seguridad de la información debe ser implantada bajo un marco de procesos orientado a la mejora continua. En este sentido, la aplicación del R.D. 3/2010 requiere la revisión formal a través de las auditorías periódicas y la corrección de las desviaciones detectadas para garantizar que las medidas de seguridad son eficaces y proporcionan el nivel de seguridad deseado.

4.5 Responsabilidad

Todo el personal de la APC es responsable de garantizar la seguridad de los sistemas de información con diferentes grados de participación según las funciones o atribuciones asignadas. Esta responsabilidad se concreta en el cumplimiento del marco normativo en materia de seguridad y protección de datos de carácter personal que la APC haya publicado y distribuido entre el personal. El personal de la APC debe ser consciente de la necesidad de garantizar la seguridad de los sistemas de información y qué ellos son un elemento esencial para el mantenimiento y mejora de la seguridad.

5 Marco legal

Para la elaboración del contenido de la presente política de seguridad se ha tenido en consideración entre otras, la siguiente legislación:

Código Penal

- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Administración electrónica

- Ley 39/2015, de Procedimiento Administrativo Común.
- Ley 40/2015, de Régimen Jurídico del Sector Público.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- 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.002).
- Ley 59/2003 de firma electrónica.
- 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 951/2015, de 23 de octubre, de modificación del 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.

Protección de Datos de Carácter Personal

- 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.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)
- Ley 2/2011, de 4 de marzo, de Economía Sostenible.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

Propiedad Intelectual

- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 17/2001, de 7 de diciembre, de Marcas.
- Ley 20/2003, de 7 de julio, de protección jurídica del diseño industrial.

Protección de Infraestructuras Críticas y Seguridad de las Redes y Sistemas de Información.

- Ley 8/2011 por la que se establecen medidas para la Protección de las Infraestructuras Críticas.
- R.D. 704/2011 por la que se aprueba el Reglamento para la Protección de las Infraestructuras Críticas.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, más conocida como Directiva NIS.
- Real Decreto 1617/2007, de 7 de diciembre, por el que se establecen medidas para la mejora de la protección de los puertos y del transporte marítimo.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

6 Organización de la seguridad de la información

Para garantizar que todas las etapas del ciclo de vida de protección de la información sean realizadas de manera apropiada y las responsabilidades para su ejecución sean asignadas adecuadamente, la APC debe establecer una estructura jerárquica promover la aplicación consistente de la presente política y

acomodar efectivamente los frecuentes cambios tecnológicos y organizacionales.

El modelo de responsabilidades propuesto en la APC atiende a criterios de separación de tareas, eficiencia, límites en el alcance del control, autoridad, conocimientos técnicos y aplicabilidad efectiva. Las distintas funciones se segmentan para establecer una jerarquía de responsabilidades acorde con las tareas que serán asumidas por los diferentes roles. La responsabilidad legal y la especificación de las necesidades o requisitos corresponderá al Comité de Seguridad en pleno que ejercerá las funciones a nivel de gobierno. La supervisión corresponderá en sus diferentes ámbitos de actuación al Responsable de Seguridad de la Información, al Delegado de Protección de Datos y al Responsable de Seguridad y Enlace que ejercerán las funciones a nivel ejecutivo. La operación de los sistemas de información (IT y OT) que corresponde a la figura del Responsable del Sistemas (IT y OT) y Administrador de Seguridad que ejercerán las funciones a nivel operacional.

Tal como establece el R.D. 3/2010, es necesario dentro de la presente política, establecer los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, el procedimiento para su designación y renovación, así como la estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.

La organización interna de la seguridad debe atender a la necesidad de regular tres grandes bloques de responsabilidad: la especificación de las necesidades o requisitos, la operación del sistema de información que se atiene a aquellos requisitos y la función de supervisión de acuerdo con el principio básico del ENS "La seguridad como función diferenciada". Para ello, se definen siete roles generales relacionados con su participación en la gestión y supervisión de la seguridad de la información:

- Responsables de la información.
- Responsables de los servicios.
- Responsable de seguridad de la información.
- Delegado de protección de datos.
- Responsable de seguridad y enlace.
- Responsables de los sistemas de información
- Administrador de seguridad

La Autoridad Portuaria de Cartagena ha decidido que la figura de los responsables de información y responsables de servicios serán asumidas por el Comité de Seguridad de la Información constituido como Órgano colegiado y su régimen de funcionamiento se ajustará a las normas contenidas en los arts. 15 a 22 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

A este comité pertenecerán los responsables de las áreas de la APC relacionadas con servicios de administración electrónica. Los nombramientos de las personas que forman el Comité de Seguridad y los roles que ostentan serán definidos en el ANEXO: MIEMBROS DEL C.S.I. Y ROLES que podrá ser modificado de forma independiente al contenido de la presente política.

A continuación, se describen las funciones que tendrá este Comité y cuáles son los roles y responsabilidades que ostentarán sus miembros.

6.1 Comité de Seguridad.

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 la APC y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos de carácter personal y seguridad. Este Comité es el máximo órgano al que compete la Seguridad de la Información en la APC. En este sentido, identifica objetivos y estrategias relacionados con la protección de las instalaciones, la seguridad de la información y dirige y controla los procesos relacionados con la seguridad. El funcionamiento de este Comité se ajustará al funcionamiento de los órganos colegiados recogido en la Ley 40/2015, de Régimen Jurídico del Sector Público. Su composición estará formada por las personas que ostenten los siguientes cargos:

- El Director General.
- El Responsable de Secretaría General.
- El Responsable de Administración Electrónica.
- El Responsable de Explotación.
- El Responsable de Sistemas de Información.
- El Responsable de Infraestructuras.
- El Responsable de Instalaciones.
- El Responsables de Seguridad de la Información. IT - OT
- El Responsable de Seguridad y Enlace.
- El Delegado de Protección de Datos.
- El Administrador de Seguridad

Una de estas personas actuará como secretario del Comité (el Responsable de Seguridad de la Información). Este Comité podrá en convocatorias concretas ampliarse a otros responsables de la APC cuando así lo considere necesario el responsable de seguridad. También podrán asistir a sesiones del Comité de Seguridad en calidad de asesores las personas que en cada caso se estimen pertinentes. El Comité de Seguridad de la Información será formalmente constituido con la aprobación de la presente Política y el nombramiento de los

cargos será efectivo con la aprobación de dicho documento. El nombramiento se revisará cuando cualquiera de los cargos del Comité quede vacante. El Comité de Seguridad, se reunirá con carácter ordinario, al menos una vez semestralmente, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

Son funciones del Comité de Seguridad las siguientes:

- Identificar los objetivos de la APC en el ámbito de la Seguridad de la Información.
- Elaborar la Política de Seguridad, establecer los criterios de revisión de la misma, revisarla, distribuirla y velar por su cumplimiento.
- Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en la APC.
- Establecer los requisitos de seguridad que deben cumplir a nivel organizativo, técnico y de control, los sistemas y servicios de la APC.
- 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.
- Aprobar los nombramientos de responsables y responsabilidades en materia de seguridad de la información.
- Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la Política de Seguridad.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de las Administraciones en materia de Seguridad.
- Promover la formación y concienciación en materia de Seguridad de la Información a todo el personal.
- 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 la APC.
- Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en la APC.
- Establecimiento de los requisitos de la información en materia de seguridad.

6.2 Roles, funciones y responsabilidades en materia de seguridad.

Responsables de la información.

Esta responsabilidad recaerá en el Comité de Seguridad, que constará de un presidente, un secretario y de los titulares de los órganos o unidades administrativas que gestionen cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos de los que sea responsable. Los Responsables de la información tendrán las siguientes funciones:

- 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.
- Trabajar en colaboración con el responsable de seguridad y el del sistema en el mantenimiento de los servicios de administración electrónica catalogados.
- Apoyar la realización de los análisis de riesgos y valorar las diferentes opciones de gestión del riesgo a implantar.
- Valorar y decidir, junto con los Responsables de los Servicios, 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.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes que puedan tener acceso a información de los procedimientos administrativos que gestiona y realizar el seguimiento de su cumplimiento.

Responsables de los servicios.

Esta responsabilidad recaerá en el Comité de Seguridad, que constará de un presidente, de un secretario y de los titulares de los órganos o unidades administrativas que gestionen el servicio, pudiendo una misma persona acumular las responsabilidades de la información de todos los servicios de los que sea responsable. Los Responsables de los servicios tendrán las siguientes funciones:

- 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.
- Trabajar en colaboración con el responsable de seguridad y el del sistema en el mantenimiento de los servicios de administración electrónica catalogados.

- Apoyar la realización de los análisis de riesgos y valorar las diferentes opciones de gestión del riesgo a implantar.
- Valorar y decidir, junto con los Responsables de los Servicios, 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.
- Velar por la inclusión de cláusulas sobre seguridad en los contratos con terceras partes que puedan afectar a sus servicios y realizar el seguimiento de su cumplimiento.

Responsables de los sistemas de información.

Los Responsables de los sistemas de información, dentro de sus áreas de actuación, tendrán asignadas las siguientes funciones:

- Desarrollo, operación y mantenimiento de los sistemas de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de la Seguridad de la Información.
- Atender las necesidades de seguridad identificadas en el análisis de riesgos tanto sobre los sistemas de información (Entornos IT) como sobre los entornos de informática industrial (Entornos OT).
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.
- Elaborar procedimientos técnicos de seguridad de los sistemas de información sobre los entornos IT y OT.
- Elaborar planes de continuidad de los sistemas de información.
- Colaborar para la realización del análisis de riesgos de los sistemas de información tanto de los entornos IT como OT.
- Implementar, gestionar y mantener las medidas de seguridad aplicables al sistema de información.
- 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.
- 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.
- Aprobar los cambios en la configuración vigente del sistema de información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- 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.

- Informar al Responsable de Seguridad de la Información o Responsable de Seguridad y Enlace de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Responsable de seguridad de la información.

El Responsable de seguridad de la información de la APC tendrá las siguientes funciones:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la organización.
- Asesorar en materia de seguridad a los integrantes de la APC que así lo requieran.
- Coordinar la interacción con otros organismos especializados en materia de gestión de incidentes de ciberseguridad.
- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
- 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 – Medidas de Seguridad del ENS.
- 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.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la APC en materia de seguridad.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.
- Elaboración de la normativa de seguridad de la APC.
- Aprobación de los procedimientos de seguridad elaborados por el Responsable del Sistemas de Información.

El Responsable de Seguridad podrá designar cuantos Administradores de Seguridad delegados considere necesarios. Los administradores de seguridad se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de Seguridad teniendo dependencias funcionales directas con él. El Responsable de Seguridad deberá reportar directamente a la Dirección o al Comité de Seguridad y será nombrado y cesado por éste.

Delegado de Protección de Datos.

El Delegado de Protección de Datos de la APC tendrá las siguientes funciones:

- Asesorar en materia de protección de datos a los integrantes de la APC que así lo requieran.
- Supervisar la adecuada gestión de riesgos en materia de privacidad y asegurar un adecuado nivel de protección a los tratamientos de datos de carácter personal realizados por la APC.
- Coordinar la interacción con otros organismos especializados y la AEPD.
- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad cuando estas impliquen datos de carácter personal y tenga que valorarse la necesidad de notificación.
- 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 de la Información.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad de la Información.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la APC en materia de privacidad.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.
- Elaboración de la normativa de protección de datos de la APC.
- Aprobación de los procedimientos de seguridad vinculados con el cumplimiento de la legislación en materia de Protección de Datos elaborados por el Responsable del Sistema.

El Delegado de Protección de Datos será nombrado y notificado a la AEPD.

Responsable de Seguridad y Enlace.

El Responsable de Seguridad y Enlace asumirá también la figura de Delegado de Seguridad de la Infraestructura Crítica y tendrá las siguientes funciones:

- Representar al Operador Crítico ante la Secretaría de Estado de Seguridad en todas las materias relativas a la seguridad de sus infraestructuras y los diferentes planes especificados en este reglamento.
- Canalizar las necesidades operativas e informativas que surjan.
- Identificar, analizar y evaluar las situaciones de riesgo que puedan afectar a la vida e integridad de las personas y al patrimonio.
- Planificar, organizar y controlar las actuaciones precisas para la implantación de las medidas conducentes a prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza con medios y medidas precisas, mediante la elaboración y desarrollo de los planes de seguridad aplicables.
- La comunicación a las Fuerzas y Cuerpos de Seguridad competentes de las circunstancias o informaciones relevantes para la seguridad ciudadana, así como de los hechos delictivos de los que tenga conocimiento en el ejercicio de sus funciones.
- Asesorar en materia de seguridad física a los integrantes de la APC que así lo requieran.
- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.
- Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos para la protección de las infraestructuras calificadas como servicios esenciales.
- 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.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.
- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de la APC en materia de protección de infraestructuras críticas.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.
- Elaboración de la normativa de seguridad de la APC.

- Aprobación de los procedimientos de seguridad de los que sea autoridad competente.

El Responsable de Seguridad y Enlace podrá designar cuantos Administradores de Seguridad delegados considere necesarios. Los administradores de seguridad se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de Seguridad teniendo dependencias funcionales directas con él. El Responsable de Seguridad y Enlace será nombrado y cesado por el Comité de Seguridad.

Administrador de seguridad.

Los responsables de seguridad (Seguridad y Enlace o Seguridad de la Información) podrán delegar actividades en la figura de los Administradores de Seguridad y tendrá las siguientes funciones:

- Implementar, gestionar y mantener las medidas de seguridad aplicables a las infraestructuras o los sistemas de información.
- Gestionar, configurar o actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.
- Gestionar las autorizaciones y privilegios concedidos a los usuarios del sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Aplicar los Procedimientos Operativos de Seguridad (POS).
- Asegurar que los controles de seguridad establecidos son eficaces y se cumplen los procedimientos aprobados.
- 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.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de la Seguridad y Enlace o al Responsable de Seguridad de la Información de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

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 Responsable de Seguridad y Enlace.

6.3 Asesoramiento especializado en materia de seguridad

El Responsable de Seguridad será el encargado de coordinar los conocimientos y las experiencias disponibles en la APC con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos o entidades externas cuando lo considere necesario.

7 Obligaciones del Personal de la APC.

Todo el personal de la APC, 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. Se establecerá un programa de concienciación continua para atender a todos los miembros de la APC, en particular a los de nueva incorporación. Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo.

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.

8 Desarrollo del marco normativo.

8.1 Estructura del marco normativo.

La Autoridad Portuaria ha establecido un marco normativo en materia de seguridad que se encuentra estructurado por diferentes niveles. Esta jerarquía de documentos debe ser conexa y coherente para dar cumplimiento a las medidas de seguridad establecidas por 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.

La Autoridad Portuaria estructura su marco normativo en los siguientes tipos de documento:

- La presente ***política de seguridad de la información*** que establece los requisitos y criterios de protección en el ámbito de la APC y servirá de guía para la creación de normas de seguridad.
- Las ***normas de seguridad de la información*** definen qué hay que proteger y los requisitos de seguridad deseados. El conjunto de todas las normas de seguridad debe cubrir la protección de todos los entornos de los sistemas de información de la organización y determinan los requisitos que deben ser alcanzados para poder satisfacer y cumplir cada uno de los objetivos de seguridad establecidos en la política.
- Los **procedimientos de seguridad** en los que describirá de forma concreta cómo proteger lo definido en las normas y las personas o grupos responsables de la implantación, mantenimiento y seguimiento de su nivel de cumplimiento. Estos documentos especifican cómo llevar a cabo las tareas habituales, quién debe hacer cada tarea y cómo identificar y reportar comportamientos anómalos.

8.2 Revisión, aprobación y difusión del marco normativo de seguridad

La documentación perteneciente al marco normativo en materia de seguridad debe estar controlada para garantizar su uso adecuado y correcto. Por ello, es necesario determinar en el presente apartado cómo se realizarán las siguientes tareas:

- Aprobar en forma los documentos previamente a su distribución.
- Revisar, actualizar y volver a aprobar los documentos, según vaya siendo necesario.
- Asegurar que los documentos están disponibles para todo aquel que los necesite.
- Asegurar que la distribución de documentos está controlada.
- Prevenir el uso no intencionado de documentos obsoletos.

La aprobación de los diferentes documentos del marco normativo se realizará según su tipo y se delegará en los diferentes roles establecidos dentro del organigrama de la APC encargado de velar por la seguridad de la información. Los diferentes tipos de documento se regirán por el siguiente criterio de aprobación:

- *Política de seguridad* será aprobada por el Comité de Seguridad. El Responsable de seguridad será encargado de realizar la propuesta de actualización cuando lo considere necesario.
- *La Normativa de seguridad también será aprobada por* el Comité de Seguridad.
- *Los Procedimientos de seguridad* serán aprobados bien por el Comité de Seguridad o bien por el Responsable de Seguridad y Enlace o el

Responsable de Seguridad de la Información según el alcance de los procedimientos y las áreas o departamentos afectados. Cualquier procedimiento técnico cuyo alcance sean los sistemas de información podrá ser aprobado directamente por los correspondientes Responsables de seguridad o los Responsables de los sistemas de información afectados.

La revisión y propuesta de nuevas versiones del marco normativo podrá ser realizada por cualquiera de las áreas afectadas de la APC y notificada al Responsable de seguridad y enlace o Responsable de Seguridad de la Información que canalizará las propuestas a través del Comité de Seguridad de la Información para que sean aprobadas por el Órgano adecuado según el criterio establecido en el párrafo anterior.

La publicación de la política estará localizable en los recursos tecnológicos accesibles a todos los empleados y terceros que participen de cualquiera de las actividades en materia de administración electrónica de la APC. La normativa y los procedimientos de seguridad deberán estar accesibles según los requisitos de control de acceso para que sean consultables por el personal que deba garantizar su cumplimiento.

9 Cooperación con otras Administraciones.

A efectos de intercambiar experiencias y obtener asesoramiento para la mejora de las prácticas y controles de seguridad, la APC mantendrá contactos periódicos con otras Administraciones Públicas y Organismos creados para dar soporte a la Estrategia de Ciberseguridad Nacional así como empresas especializadas en temas de seguridad de la información y firmará cuantos acuerdos o convenios considere necesario para disponer de información actualizada y relevante que permita una mayor protección de los sistemas de información.

10 Terceras Partes

La contratación de servicios externos que se vean afectados por el marco de cumplimiento establecido por la Legislación en materia de protección de infraestructuras críticas, administración electrónica o protección de datos (RGPD), deberá satisfacer la normativa en materia de contratación y acuerdos de nivel de servicio. La APC pondrá a disposición del tercero tanto la política como los documentos del marco normativo que deba cumplir la prestación de dichos servicios. Dicha tercera parte quedará sujeta a las obligaciones establecidas por la normativa pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias para que exista un canal directo de notificación, debiendo ser designado un responsable de seguridad que coordine

cualquier incidente que pueda afectar a la APC estando implicado o siendo causado por este tercero.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere 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. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

11 Aprobación y entrada en vigor

Texto aprobado el día 25 de Febrero de 2021 por el Comité de Seguridad de la Información de la Autoridad Portuaria de Cartagena. Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva versión.

Firmado por 06985834K FERMIN ROL (R: Q3067007I) el día 17/03/2021 con un certificado emitido por AC CAMERFIRMA FOR NATURAL PERSONS - 2016