ÍNDICE:

1. Aprobación y entrada en vigor

Documento aprobado por el Consejo de Administración de la Autoridad Portuaria de Avilés en sesión celebrada con fecha 20 de noviembre de 2018.

Esta "Política de Seguridad de la Información", en adelante Política, será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. Introducción

La Autoridad Portuaria de Avilés depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la seguridad 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 de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad 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. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, 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.
De este modo, todas los departamentos, divisiones y unidades de la Autoridad Portuaria, tienen presente 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.
Por tanto, para la Autoridad Portuaria, 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 para detectar cualquier incidente y reaccionando con presteza a los incidentes para recuperarse lo antes posible, acorde a lo establecido en el Artículo 7 del ENS.

3. Misión de la Autoridad Portuaria

La misión de la Autoridad portuaria consiste en facilitar a los agentes económicos servicios portuarios eficientes, impulsando el desarrollo económico del entorno, dentro de un marco de crecimiento sostenible, todo ello en el marco de sus competencias.

Las competencias de la Autoridad Portuaria de Avilés se recogen en 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 de la Marina Mercante, publicado en el BOE núm. 253, de 20 de octubre de 2011.

4. Alcance

Esta Política se aplicará a los sistemas de información de la Autoridad Portuaria relacionados con el ejercicio de sus competencias y a todos los usuarios con acceso autorizado a los mismos, sean o no empleados públicos y con independencia de la naturaleza de su relación jurídica con la Autoridad Portuaria de Avilés. Todos ellos tienen la obligación de conocer y cumplir esta “Política de Seguridad de la Información” y la normativa de seguridad, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue al personal afectado.

5. Marco normativo

El marco normativo en que se desarrollan las actividades de la Autoridad Portuaria, y, en particular, la prestación de sus servicios electrónicos, está integrado por las siguientes normas:

- 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.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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).
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- 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.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- 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.
- 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.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- 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 de la Marina Mercante.
- Real Decreto 145/1989, de 20 de enero. Se aprueba el Reglamento de Admisión, Manipulación y Almacenamiento de Mercancías Peligrosas en los Puertos.
- Boletín Oficial del Estado nº 189 de 8 de agosto de 2011, por el que se aprueba la Resolución de 18 de julio de 2011, de la Autoridad Portuaria de Avilés, por el que se crea la Sede Electrónica de la Entidad.
- Boletín Oficial del Estado nº 189 de 8 de agosto de 2011, por el que se aprueba la Resolución de 18 de julio de 2011, de la Autoridad Portuaria de Avilés y por la que se crea y regula el registro electrónico de la Entidad.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica de la Autoridad Portuaria derivadas de las anteriores y publicadas en la sede electrónica comprendidas dentro del ámbito de aplicación de la presente Política.

El mantenimiento del marco normativo será responsabilidad del Comité de Seguridad de la Información y se mantendrá en un Anexo a este documento. Incluido las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el “Artículo 29. Instrucciones técnicas de seguridad y guías de seguridad”.
Así mismo, el Comité también será responsable de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

6. Cumplimiento de Artículos

La Autoridad Portuaria para lograr el cumplimiento de los artículos 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, que recogen los principios básicos y de los requisitos mínimos, ha implementado diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

Seguridad como un proceso integral (artículo 6) y seguridad por defecto (artículo 19)

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Los sistemas se diseñarán de forma que garanticen la seguridad por defecto, del siguiente modo:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) En un sistema 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.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Reevaluación periódica (artículo 9) e integridad y actualización del sistema (Artículo 20)

La Autoridad Portuaria ha implementado controles y evaluaciones regulares de la seguridad, (incluyendo evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de seguridad de la seguridad de los sistemas en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán de una autorización formal.

Así mismo, solicitará la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

Gestión de personal (artículo 14) y profesionalidad (artículo 15)

Todos los miembros de la Autoridad Portuaria, que se encuentran dentro del ámbito del ENS, atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la Autoridad Portuaria, en particular al 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. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su

primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Gestión de la seguridad basada en los riesgos (artículo 6) y análisis y gestión de riesgos (artículo 13)

Todos los sistemas afectados por esta Política están sujetos a un análisis de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de Seguridad ENS será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.
El proceso de gestión de riesgos comprenderá las siguientes fases:

1. Categorización de los sistemas.
2. Análisis de riesgos.

El Comité de Seguridad procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

Las fases de este proceso se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional.
En particular, para realizar el análisis de riesgos se utiliza la metodología MAGERIT - metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica (MAGERIT figura en el inventario de métodos de análisis y gestión de riesgos de ENISA).

Incidentes de seguridad (artículo 24), prevención, reacción y recuperación (artículo 7)

La Autoridad Portuaria ha implementado un proceso integral de detección, reacción y recuperación frente a código dañino mediante el desarrollo de procedimientos que cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y

resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.
Para que la información y/o los servicios no se vean perjudicados por incidentes de seguridad, la Autoridad Portuaria implementa las medidas de seguridad establecidas por el ENS, así como cualquier otro control adicional, que haya identificado como necesario, a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente.
La Autoridad Portuaria establecerá las siguientes medidas de reacción ante incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Para garantizar la disponibilidad de los servicios, la Autoridad Portuaria dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.

Líneas de defensa (artículo 8) y prevención ante otros sistemas interconectados (artículo 22)

La Autoridad Portuaria ha implementado una estrategia de protección basada en múltiples capas, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una de las capas falle, el sistema implementado permita:

a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
a) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
b) Minimizar el impacto final sobre el mismo.

Esta estrategia de protección ha de proteger el perímetro, en particular, si se conecta a redes públicas. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Función diferenciada (artículo 10) y organización e implantación del proceso de seguridad (artículo 12)

La Autoridad Portuaria ha organizado su seguridad comprometiendo a todos los miembros de corporación, mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

Autorización y control de los accesos (artículo 16)

La Autoridad Portuaria ha implementado mecanismos de control de acceso al sistema de información, limitándolos a los estrictamente necesarios y debidamente autorizados.

Protección de las instalaciones (artículo 17)

La Autoridad Portuaria ha implementado mecanismo de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad (artículo 18)

La Autoridad Portuaria tendrá en cuenta, para la adquisición de productos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.

Protección de la información almacenada y en tránsito (artículo 21) y continuidad de la actividad (artículo 25)

La Autoridad Portuaria dispone de mecanismos para proteger la información almacenado o en tránsito especialmente cuando esta se encuentra en entornos inseguros (portátiles, tablets, soportes de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

También ha desarrollado procedimientos que aseguran la recuperación y conservación a largo plazo de los documentos electrónicos producidos en el ámbito de sus competencias. De igual modo, dispone de mecanismos de seguridad correspondientes a la naturaleza del soporte en que se encuentren, para garantizar que toda información en soporte no electrónico relacionada, estará protegida con el mismo grado de seguridad que la electrónica.

Registros de actividad (artículo 23)

La Autoridad Portuaria ha habilitado registros de la actividad de los usuarios reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa. Todo ello con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación.

7. Organización de la seguridad

7.1. Criterios utilizados para la Organización de la Seguridad de la Información

La Autoridad Portuaria, teniendo en cuenta 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 y las pautas establecidas en la Guía *CCN-STIC-801 "Responsabilidades y Funciones en el ENS"*, para organizar la seguridad de la información emprenderá las siguientes acciones:

- **Designará roles de seguridad:** Responsables de Servicios, Responsables de Información, Responsable de Seguridad Física, Responsable de Seguridad de la Información, y Responsable del Sistema.
- **Constituirá un órgano consultivo y estratégico para la toma de decisiones en materia de Seguridad de la Información**. Este órgano se constituirá como un órgano colegiado y se denominará Comité de Seguridad de la Información. Será presidido por una persona física que será la que asumirá la responsabilidad formal de sus actos.

7.2. Roles y Órganos de Seguridad de la Información de la Autoridad Portuaria

En la Autoridad Portuaria los roles y órganos de seguridad de la información, son representados por los siguientes:

- **Responsables de los Servicios y Responsables de la Información ENS**: han sido designados por el Consejo de Administración y son personas con alto cargo en la organización y que se encuentren directamente relacionados con el servicio y/o información de la cual serán responsables.
- **Delegado de Protección de Datos:** Responsable Departamento Secretaria General.

- **Responsable de Seguridad ENS:** Jefa División de Sistemas Información y Comunicaciones.
- **Responsable del Sistema ENS:** Técnica Sistemas Información y Comunicaciones.
- **Comité de Seguridad de la Información**:
  - Presidente: Director de la Autoridad Portuaria de Avilés
  - Secretario/a: designado entres sus vocales por acuerdo del Comité
  - Vocales:
    - Responsables de Información y Servicios.
    - Delegado de Protección de Datos: Responsable Departamento Secretaría General.
    - Responsable de Seguridad ENS: Jefa División de Sistemas Información y Comunicaciones.
    - Responsable del Sistema ENS: Técnica Sistemas Información y Comunicaciones.
    - Responsable de Seguridad Física: Jefe de División de Operaciones y Servicios Portuarios.

Los Responsables de la Información y los Servicios, serán convocados en función de los asuntos a tratar, pudiendo el Comité de Seguridad recoger las funciones y obligaciones de los Responsables de la Información y los Servicios, en aquellas acciones transversales, en las que le, sea solicitado y/o se considere necesario.

Asimismo, y con carácter opcional, podrán incorporarse a las labores del Comité grupos de trabajo especializados, ya sean de carácter interno, externo o mixto.

El Comité de Seguridad de la Información celebrará sus sesiones en las dependencias de la Autoridad Portuaria con periodicidad semestral, previa convocatoria al efecto realizada por el Presidente, quien tendrá la facultad de suspender la celebración de las sesiones del Comité de Seguridad de la Información como consecuencia de los periodos vacacionales, cuando ello no suponga un menoscabo a la seguridad, así como para a posponer o adelantar la celebración de las sesiones ordinarias del Comité, dentro de la misma semana de su celebración, cuando el día fijado sea festivo.

7.3. Responsabilidades de los roles asociados al Esquema Nacional de Seguridad

Responsables de la Información y Servicios:

- Establecer y aprobar los requisitos de seguridad aplicables al Servicio (niveles de seguridad del servicio) y la Información (niveles de seguridad de la información), dentro del marco establecido en el anexo I del Real Decreto 3/2010, de 8 de enero. Pudiendo recabar una propuesta al Responsable de Seguridad ENS y teniendo en cuenta la opinión del Responsable del Sistema ENS y/o Comité de Seguridad de la Información.
- Dictaminar respecto a los derechos de acceso al Servicio y a la Información.
- Aceptar los niveles de riesgo residual que afectan al Servicio y a la Información.
- Poner en comunicación del Responsable de Seguridad ENS, cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo. El cual dará traslado de dichos cambios, al Comité de Seguridad de la Información, en su próxima reunión.

Responsable de Seguridad ENS:

- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios electrónicos prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución del análisis de riesgos, de la Declaración de Aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información.
- Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema
- Gestionar los procesos de certificación
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.

Responsable del Sistema ENS:

- Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida. Elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de Seguridad y/o Comité de Seguridad de la Información de la Información.
- Participará en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad.
- Llevar a cabo las funciones del administrador de la seguridad del sistema:
    - La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.
    - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
    - Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
    - 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 proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
    - Informar al Responsable de Seguridad 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.

Cuando la complejidad del sistema lo justifique el Responsable de Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen.

7.4. Funciones del Delegado de Protección de Datos

Las funciones del Delegado de Protección de Datos (DPD), que serán asumidas por el Comité de Seguridad de la Información, serán como mínimo:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente

Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.

- Supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento 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.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

7.5. Funciones y obligaciones del Comité de Seguridad de la Información

El Comité organiza **la Seguridad de la Información** para perseguir los siguientes objetivos:

- **Desarrollar la estrategia de seguridad de la información**. Para ello establecerá las directrices necesarias para definir los planes de seguridad de la información anuales, coordinando tanto su realización como seguimiento de ejecución.
- **Coordinar las adquisiciones y desarrollos** decidiendo inversiones, racionalizar el gasto y evitar disfunciones que debiliten el sistema que permitan ser explotados por una amenaza ya sea intencionada o no.
- **Coordinar servicios y funciones** para evitar disfunciones y maximizar así el uso.

Este Comité además tiene el objeto de dar cumplimento, entre otras obligaciones y cumplimiento legal relacionadas con la Seguridad de la Información, a las responsabilidades establecidas en el Esquema Nacional de Seguridad en el ámbito de los trámites electrónicos y a la normativa de protección de datos personales.

El Comité de Seguridad de la Información **tendrá las siguientes funciones**:

- Atender las inquietudes, en materia de Seguridad de la Información, de la Administración y de las diferentes áreas informando regularmente del estado de la Seguridad de la Información a la Dirección.
- Asesorar en materia de Seguridad de la Información, siempre y cuando le sea requerido.

- ¬ Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes roles de seguridad y/o responsables entre diferentes Departamentos, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- ¬ Recoger las funciones y obligaciones de los Responsables de la Información y los Servicios ENS, en aquellas acciones transversales, en las que le sea solicitado y/o se considere necesario.
- ¬ Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:
    - o Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
    - o Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
    - o Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación (Privacy by Design). En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
    - o Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
    - o Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
    - o Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación el Órgano Superior.
    - o Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con el Dirección General.
    - o Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
    - o Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
    - o Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
    - o Promover la realización de las auditorías periódicas ENS y de la normativa de protección de datos, que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

7.6. Procedimientos de designación

La creación del Comité de Seguridad de la Información, el nombramiento de sus integrantes y la designación de los Responsables identificados en esta política es realizada por el Consejo de Administración de la Autoridad Portuaria de Avilés y comunicada a las partes afectadas, mediante un acta de designación y de aceptación, remitida por el Director de la Autoridad Portuaria de Avilés.
Los miembros del Comité serán renovados cada cuatro años o con ocasión de vacante.

8. Datos de carácter personal

La Autoridad Portuaria solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos. Estas medidas estarán recogidas en los documentos y normativas de seguridad de seguridad que se encuentran bajo la custodia del Comité de Seguridad de la Información.

9. Desarrollo de la política de seguridad de la información

El Comité de Seguridad de la Información ha aprobado el desarrollo de un sistema de gestión, que será establecido, implementado, mantenido y mejorado, conforme a los estándares de seguridad. Este sistema se adecuará y servirá de gestión de los controles Esquema Nacional de Seguridad. El sistema será documentado y permitirá generar evidencias de los controles y del cumplimiento de los objetivos marcados por el Comité. Existirá un procedimiento de gestión documental que establecerá las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
Corresponde al Comité de Seguridad de la Información la revisión anual de la presente Política proponiendo, en caso de que sea necesario mejoras de la misma, para su aprobación por parte del concejal competente por razón de la materia de la Autoridad Portuaria.

10. Terceras partes

Cuando la Autoridad Portuaria preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. Se establecerán

canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Autoridad Portuaria utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta 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. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

Cuando algún aspecto de esta Política de Seguridad de la Información no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información ENS 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.