

26 MAR 2021

acordándose su aprobación,

EL SECRETARIO

José Ramón Costas Alonso

Asunto: Aprobación del documento de la Política de Seguridad de la Información de la Autoridad Portuaria de Vigo.

AL CONSEJO DE ADMINISTRACIÓN

Informe de la Directora

El artículo 11 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 contempla en el Anexo II de dicho Real Decreto los Requisitos mínimos de Seguridad.

En este sentido, el mencionado 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.”*

La estructura de este documento de política de seguridad de la información sigue las pautas establecidas por la guía del Centro Criptológico Nacional para garantizar la seguridad de los Sistemas de las Tecnologías de la Información y las Comunicaciones de la administración (CCN-STIC-805), para la redacción de la Política de Seguridad en el ámbito del Esquema Nacional de Seguridad.

La Política de Seguridad de la Información recoge la postura de la Autoridad Portuaria de Vigo en cuanto a la seguridad de la información y establece los criterios generales que deben regir la actividad del organismo en cuanto a esta.

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 de información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, 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.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos y de garantía de los derechos digitales (en adelante ENS y LOPD-gdd), 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 acuerdo con lo anterior, y con lo establecido en el artículo 11 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, se propone al Consejo de Administración que adopte la siguiente RESOLUCIÓN:

Aprobar del documento de la Política de Seguridad de la Información de la Autoridad Portuaria de Vigo.

En Vigo, a 22 de marzo de 2021.

LA DIRECTORA,

BEATRIZ COLUNGA
FIDALGO -
36123676Z

Prescrito digitalmente por BEATRIZ COLUNGA
FIDALGO - 36123676Z
Número de identificación DNI: 36123676Z
COLUNGA FIDALGO - 36123676Z - 36123676Z
FIDALGO - 36123676Z - 36123676Z - 36123676Z
AUTORIDAD PORTUARIA DE VIGO
INSTRUMENTO FIDUCIARIO DE FIDELIZACIÓN
PUB. CC. Verificación: https://www.puerto.vigo.es/verificacion/

Fdo. Beatriz Colunga Fidalgo.

u/cjo/informeconsejoseguridad

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

Esquema Nacional de Seguridad
Política de Seguridad de la Información
11 Marzo 2021



ELABORADO POR:	REVISADO POR:	APROBADO POR:
Ingenia	Jefe de Dpto. de Tecnologías de la APV	Consejo de Administración APV
fecha:11/03/21	fecha: 23/03/2021	fecha:26/03/2021

HISTORIAL DE CAMBIOS

NOMBRE DEL FICHERO	VERSIÓN	RESUMEN DE CAMBIOS PRODUCIDOS	FECHA
APV STIC-POL-1 Política de Seguridad de la Información v1.0.docx	1.0	Primera versión aprobada	11/03/21

CLASIFICACIÓN DEL DOCUMENTO

USO INTERNO

Nota de confidencialidad: La información contenida en este documento es confidencial y sólo se puede utilizar de acuerdo a la cláusula de CONTROL DE DISTRIBUCIÓN.

Es responsabilidad del Área o Departamento receptor de este documento su distribución interna en base a la necesidad de conocer la información aquí contenida.

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

CONTROL DE DISTRIBUCIÓN

AUTOR(ES): Ingenia

DISTRIBUCION: Autoridad Portuaria de Vigo

REFERENCIAS

TÍTULO	NOMBRE DEL FICHERO
Documentos Internos	
[1]	
Documentos Externos	
[2] RD 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica	
[3] 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.	
[4] CCN-STIC-804. Esquema Nacional de Seguridad. Guía de Implantación	
[5] CCN-STIC-821 Normas de Seguridad en el ENS y sus Anexos	

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

ÍNDICE DE CONTENIDOS

1.	APROBACIÓN Y ENTRADA EN VIGOR	5
2.	INTRODUCCIÓN	5
3.	LA AUTORIDAD PORTUARIA DE VIGO	5
4.	MARCO NORMATIVO.....	9
5.	POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN	10
6.	ALCANCE.....	11
7.	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	11
7.1	ESTRUCTURA DE ESPECIFICACIÓN	12
7.1.1	<i>Responsable de la Información</i>	12
7.1.2	<i>Responsable del Servicio</i>	12
7.1.3	<i>Responsable del Tratamiento.....</i>	12
7.2	ESTRUCTURA DE SUPERVISIÓN	13
7.2.1	<i>Responsable de Seguridad de la Información.....</i>	13
7.2.2	<i>Responsable de Seguridad Física.....</i>	14
7.2.3	<i>Delegado de Protección de Datos</i>	14
7.2.4	<i>Comité de Seguridad de la Información</i>	15
7.3	ESTRUCTURA DE OPERACIÓN	16
7.3.1	<i>Responsable de los Sistemas de Información</i>	16
7.4	DESIGNACIÓN DE ROLES DE LAS ESTRUCTURAS DE SEGURIDAD	17
7.5	MECANISMOS DE COORDINACIÓN Y DE RESOLUCIÓN DE CONFLICTOS.....	17
8.	OBLIGACIONES DEL PERSONAL	17
9.	TERCERAS PARTES.....	18
10.	FORMACIÓN Y CONCIENCIACIÓN.....	18
11.	GESTIÓN DE RIESGOS.....	19
12.	DATOS DE CARÁCTER PERSONAL	19
13.	DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	19
14.	COMPROMISO DE LA PRESIDENCIA	19
15.	REVISIÓN DE ESTA POLÍTICA	20

 Puerto de Vigo <small>Autoridad Portuaria de Vigo</small>	Política de Seguridad de la Información	Id: STIC-POL-01
		Versión: V1.0 11.03.21
ESQUEMA NACIONAL DE SEGURIDAD		

1. Aprobación y Entrada en Vigor

La presente Política de Seguridad de la Información fue aprobada por el Consejo de Administración de la Autoridad Portuaria de Vigo en sesión celebrada el día 26 de Marzo de 2021, siendo efectiva desde la mencionada fecha hasta que sea reemplazada por una nueva Política.

2. Introducción

Este documento constituye la **Política de Seguridad de la Información de la Autoridad Portuaria de Vigo**, en adelante APV, en cumplimiento del artículo 11 (Requisitos mínimos de Seguridad 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) y de la medida de seguridad org.1 contemplada en el Anexo II de dicho Real Decreto.

En este sentido, el mencionado 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."*

La estructura de este documento sigue las pautas establecidas por la guía CCN-STIC-805 para la redacción de la Política de Seguridad en el ámbito del Esquema Nacional de Seguridad.

La Política de Seguridad de la Información recoge la postura de la APV en cuanto a la seguridad de la información y establece los criterios generales que deben regir la actividad del organismo en cuanto a esta.

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 de información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, 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.

Esto implica que se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad y la Ley Orgánica de Protección de Datos y de garantía de los derechos digitales (en adelante ENS y LOPD-gdd), 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.

3. La Autoridad Portuaria de Vigo

La Autoridad Portuaria de Vigo (APV) es un Organismo de Derecho Público con personalidad jurídica y patrimonio propios que gestiona el puerto de Vigo.

La misión de la Autoridad Portuaria de Vigo (APV), como Administración pública, es la de acrecentar el valor que tiene para esta sociedad con la eficacia en el desarrollo de su actividad principal: el intercambio de mercancías mediante el transporte marítimo y terrestre.

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

El Puerto de Vigo es responsable de servir a la industria que le rodea con eficacia, transparencia y sencillez; de extender su área de influencia lo máximo posible, facilitar el comercio internacional, velar por su competitividad y capacidad de innovación, y de impulsar el empleo y el bienestar económico, social y medioambiental de su entorno.

Esta prosperidad no depende solo de una gestión portuaria eficiente, precisa, además, de infraestructuras dignas del siglo XXI que permitan hacer de Vigo un punto de comunicación intermodal moderno. Es indispensable la coordinación con el resto de los puertos gallegos para generar sinergias que propicien economías de escala, y para que se aproveche la ventaja competitiva que le ofrece a Galicia el poseer un conjunto de abrigos naturales e infraestructuras portuarias de difícil parangón en el mundo.

En cuanto a su visión, el Puerto de Vigo quiere ser la puerta del Atlántico y del Pacífico. Aspira constituirse en un puerto de referencia, tanto a nivel nacional como internacional, por la gestión excelente de todos sus procesos, la calidad y la seguridad de las instalaciones y los servicios que presta y las soluciones logísticas que aporta a la expansión comercial. Para ello debe anticiparse a las necesidades de futuro y esto no es posible sin un profundo ejercicio de reflexión estratégica que permita examinar la organización y aclarar ideas sobre el futuro que se quiere construir.

Así lo ha hecho al alinearse con la nueva filosofía comunitaria del "Crecimiento Azul" y la "Estrategia Europea para la fachada Atlántica", buscando situarse en el horizonte 2020 como modelo de competitividad, eficiencia y sostenibilidad. Este ejercicio se ha culminado con éxito gracias al entusiasmo puesto en ello por todas las partes interesadas, a quienes el Puerto de Vigo expresa su gratitud. Su participación ha sido, es y será esencial. Estas reflexiones se han plasmado en el proyecto "Crecimiento Azul - Puerto de Vigo 2020" que ha sido presentado y objeto de felicitación por las Autoridades comunitarias.

El mundo que nos espera requiere que consideremos todo lo que puede ser necesario en el futuro para el progreso y el crecimiento sostenible de nuestra economía. En la realidad económica de globalización que nos rodea, esto solo será posible si se asume que la iniciativa privada es el motor principal del progreso económico y que éste, una vez generado, permite redistribuir la riqueza y propiciar y mantener el estado de bienestar.

Quienes tienen responsabilidades desde la Administración pública deben favorecer el espíritu empresarial y la inversión privada. Tan es así que el propio presidente de la Comisión Europea, Jean-Claude Juncker, ha apostado por movilizar la inversión privada y generar crecimiento con el apoyo de una mayor eficiencia en la aplicación de los fondos públicos.

El Puerto de Vigo es muy especial. Todo lo que en él se descarga se transforma en la industria del entorno, y todo lo que sale embarcado ha sido en su mayoría fabricado o elaborado en su área de influencia. Esta característica hace que deba adaptarse constantemente para favorecer la competitividad de la industria de su territorio y la actividad de la inversión privada.

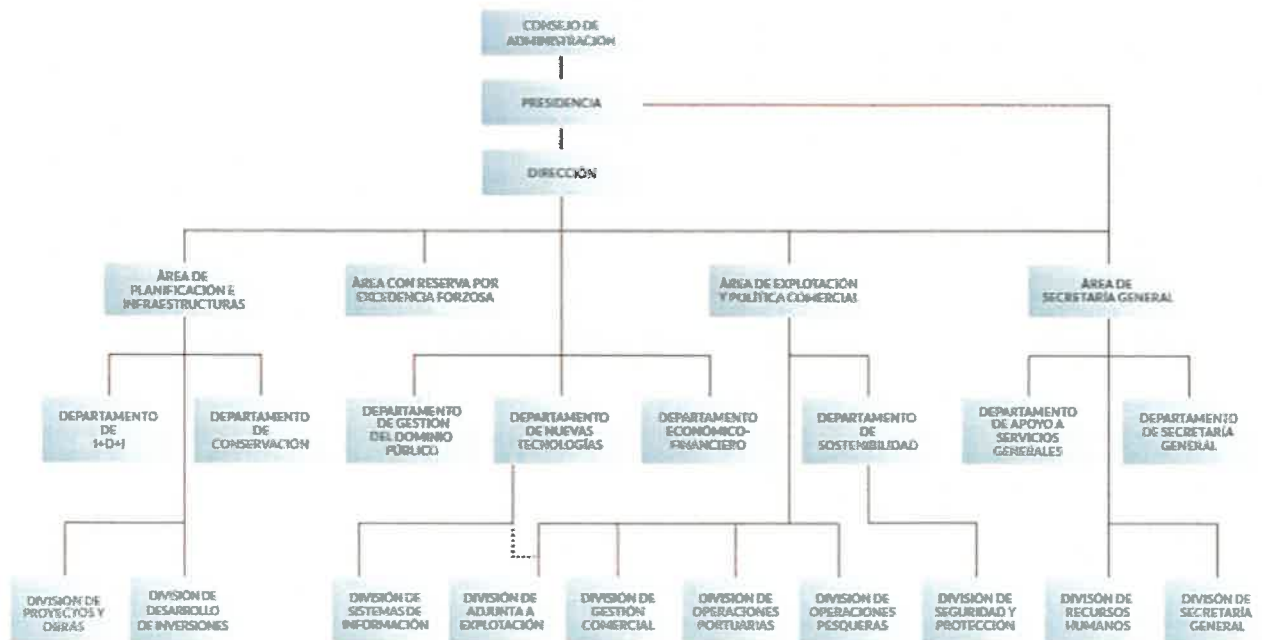
Los valores que sustentan la dirección estratégica y la gestión de la actividad cotidiana del Puerto de Vigo para lograr sus objetivos están en línea con los Objetivos de Desarrollo Sostenible y con las recomendaciones que, en este sentido, ha elaborado Puertos del Estado. Se promueven a través de proyectos y acciones en seis dimensiones:

- Institucional: buscando la conectividad en un sentido amplio, desde el desarrollo de medios e infraestructuras de transporte marítimo intermodal a la digitalización y automatización de los procesos industriales y logísticos. Proporcionando servicios de calidad, eficientes y seguros. Comprometiéndose con la transparencia y la integridad en el desempeño profesional, y en la comunicación entre la comunidad portuaria y sus grupos de interés, para favorecer el establecimiento de vínculos firmes y el sentimiento de pertenencia.

- **Económica:** integrando los intereses y preocupaciones de sus clientes y las expectativas de los mercados objetivos, defendiendo el buen funcionamiento de un mercado en libre competencia que contribuya al desarrollo socioeconómico de Vigo y su área de influencia.
- **Social:** enfocándose a las personas e implicándose con la formación para el empleo y las nuevas profesiones, con la igualdad de oportunidades y la inclusión, con la atracción de talento y su desarrollo, con la seguridad y la salud. Propiciando una mayor integración del puerto con la ciudad de Vigo mediante la maximización del dividendo social.
- **Ambiental:** protegiendo y conservando la ría y su entorno, haciendo un uso responsable de los recursos naturales y practicando la eficiencia energética. Luchando contra el cambio climático mediante el desarrollo de tráficos menos contaminantes, el fomento de las energías renovables, y el impulso a la intermodalidad, en línea con las actuales políticas de transporte de la Unión Europea.
- **Innovadora:** integrada en un sistema de conocimiento, I+D+i y transferencia, y con actuaciones comerciales diferenciadoras.

La legislación portuaria establece los parámetros de composición del Consejo de Administración y Órganos Asesores asegurando que éstos cumplan una función representativa de los intereses locales, autonómicos y nacionales, empresariales y sindicales. De este modo, los principales grupos de interés de la APV están representados en el máximo órgano de gobierno del Organismo. Debe señalarse que las autoridades portuarias son organismos públicos adscritos al Ministerio de Fomento y, como tales, están alineados con la política general que fija el Ministerio.

La estructura organizativa se muestra a continuación:



En cuanto a servicios, los servicios que prestan los puertos españoles están regulados por lo dispuesto en el Título VI del TRLPEMM. Se clasifican en generales, comerciales, de señalización marítima y portuarios.

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

Son **servicios generales** la ordenación, coordinación y control del tráfico portuario, tanto marítimo como terrestre, y los servicios de alumbrado y limpieza habitual de las zonas comunes en tierra y agua.

Los **servicios comerciales** son los que, vinculados a la actividad portuaria, no están relacionados con las operaciones portuarias y no son prestados por las autoridades portuarias. En el Puerto de Vigo solo existe el de pesaje de vehículos a terceros. Se está trabajando en la mejora de la consignación de buques y mercancías, reparación de buques, transporte y suministro de combustibles y aceites, prevención y lucha contra la contaminación y en el de entrega y recepción.

El **servicio de señalización marítima**, que está gestionado por la APV y tiene por objeto la instalación, mantenimiento, control e inspección de los dispositivos visuales, acústicos, electrónicos o radioeléctricos, destinados a mejorar la seguridad de la navegación, y los movimientos de los buques en el litoral, y en su caso, confirmar la posición de los buques en navegación.

Los **servicios portuarios** están dirigidos a hacer posible la realización de las operaciones asociadas con el tráfico marítimo en condiciones de seguridad, eficiencia, regularidad, continuidad y no discriminación. Son, por tanto, los más relevantes para el buen desarrollo del tráfico comercial del puerto. Tienen ciertas obligaciones de servicio público y una regulación más específica en el TRLPEMM. Su prestación se lleva a cabo por la iniciativa privada tras la obtención de la correspondiente licencia. Los principales son:


- Servicios técnico-náuticos: de practicaje, remolque portuario, amarre y desamarre.
- Servicios al pasaje: comprende el embarque y desembarque de pasajeros, la carga y descarga de equipajes y de vehículos en régimen de pasaje.
- Servicio de recepción de desechos generados por buques: que incluye todos los regulados en los anexos I, IV, V o VI del Convenio MARPOL 73/78.
- Servicio de manipulación de mercancías: consistente en la carga, estiba, descarga, desestiba, tránsito marítimo y transbordo de las mercancías.

Los servicios portuarios se desarrollan como actividades de interés general, en unas óptimas condiciones de seguridad, calidad, eficacia y eficiencia, y bajo unos rigurosos principios de regularidad, continuidad y no discriminación en su explotación.

El Puerto de Vigo destaca por la calidad y el personal altamente cualificado de los servicios portuarios que gestiona. Todos ellos disponen de la certificación de calidad ISO-EN-UNE9001, y de gestión medioambiental ISO-EN-UNE14001.

La APV ha puesto en marcha varias iniciativas para garantizar la transparencia en las condiciones para operar en el puerto:

- Regular las condiciones de prestación de los servicios generales.
- Realizar jornadas informativas.
- Actualizar la página web para facilitar en ella: la información sobre los pliegos reguladores de los servicios portuarios.
 - toda la documentación necesaria para los operadores interesados
 - el servicio "perfil del contratante"
 - un servicio de atención al cliente con compromiso de respuesta.
 - la tramitación a través de la sede electrónica.

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

4. Marco Normativo

La normativa a la que se encuentra sometida la Autoridad Portuaria de Vigo, más relacionada con su actividad, se recoge a continuación (por orden cronológico ascendente):

- Real Decreto 371/1987, de 13 de marzo, por el que se aprueba el Reglamento para la ejecución del Real Decreto-ley 2/1986, de 23 de mayo, de estiba y desestiba.
- Ley 22/1988, de 28 de julio, de Costas
- Real Decreto 145/1989, de 20 de enero, por el que se aprueba el Reglamento Nacional de Admisión, Manipulación y Almacenamiento de Mercancías Peligrosas en los Puertos.
- Real Decreto 393/1996, de 1 de marzo, por el que se aprueba el Reglamento general de Practicaje, de conformidad con lo establecido en la Ley de Puertos del Estado y de la Marina Mercante.
- Real Decreto 230/1998, de 16 de febrero, por el que se aprueba el Reglamento de explosivos.
- CÓDIGO INTERNACIONAL para la protección de los buques y de las instalaciones portuarias (Código PBIP), adoptadas el 12 de diciembre de 2002 mediante Resolución 2 de la Conferencia de Gobiernos contratantes del Convenio Internacional para la Seguridad de la Vida Humana en el Mar, 1974.
- Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.
- RESOLUCIÓN de 11 de octubre de 2006, de Puertos del Estado, por la que se dispone la publicación del acuerdo de su Consejo Rector, relativo a la aprobación del Pliego regulador del servicio portuario básico de amarre y desamarre de buques.
- 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.
- ORDEN FOM/938/2008, de 27 de marzo, que aprueba el pliego de condiciones generales para el otorgamiento de concesiones en el dominio público portuario estatal.
- Orden FOM/4003/2008, de 22 de julio, por la que se aprueban las normas y reglas generales de los procedimientos de contratación de Puertos del Estado y Autoridades Portuarias.
- 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.
- 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 Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.
- Orden FOM/1698/2013, de 31 de julio, por la que ese modifica la Orden FOM/4003/2008, de 22 de julio, por la que se aprueban las normas y reglas generales de los procedimientos de contratación de Puertos del Estado y Autoridades Portuarias.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Orden HAP/2425/2013, de 23 de diciembre, por la que se publican los límites de los distintos tipos de contratos a efectos de la contratación del sector público a partir del 1 de enero de 2014.
- Real Decreto-ley 8/2014, de 4 de julio, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

- Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público.
- 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 Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

5. Política General de Seguridad de la Información

El objeto de la presente Política es establecer la postura de la APV respecto a la Seguridad de la Información que afecta a los procesos relacionados con el desempeño de sus funciones y, muy particularmente, con los relacionados con la administración electrónica, tanto desde el punto de vista de los usuarios de los servicios, como desde el punto de vista interno, para la gestión del propio Organismo, así como la seguridad de la información relacionada con la operación de las infraestructuras de tecnologías de la información bajo su responsabilidad.

La APV utiliza las Tecnologías de la Información y las Comunicaciones para prestar sus servicios y es consciente de la amenaza que supone la ocurrencia de incidentes de seguridad, ya sean provocados o fortuitos, para lograr sus objetivos y la prestación de dichos servicios. Asimismo, también es consciente de que los incidentes de seguridad pueden estar provocados desde lugares remotos, a través de las conexiones a redes de comunicaciones de las que se dispone y, muy concretamente, a través de las conexiones a la internet (ciber-ataques).

La política de la APV es la de contrarrestar las amenazas mencionadas anteriormente con los medios suficientes, dentro de las posibilidades presupuestarias. Para este fin, se establecerá una estructura de seguridad, junto con los mecanismos apropiados para su gestión, y un conjunto de instrumentos de apoyo de forma que se garantice:

- el cumplimiento de los objetivos de su misión y de prestación de servicios
- el cumplimiento de la legislación y normativa aplicables
- la protección de las infraestructuras de tecnologías de la información frente a ataques deliberados

Para ello,

- se preverán y desplegarán medidas para evitar incidentes de seguridad que pudieran afectar al cumplimiento de objetivos o poner en riesgo las infraestructuras de tecnologías de la información.
- se diseñarán medidas de respuesta ante incidentes de seguridad, física o lógica, de forma que se minimice el impacto de los mismos, en caso de que ocurrieran.

Como norma general, se tendrá un enfoque de orientación al riesgo a la hora de diseñar las medidas de seguridad necesarias, poniendo más foco y esfuerzo en la mitigación de lo que suponga un mayor riesgo.

<p>CLASIF: USO INTERNO</p>	<p>Pag 10 de 20</p>	<p>APV STIC-POL-1 Política de Seguridad de la Información v1.0.docx</p>
-----------------------------------	----------------------------	--------------------------------------------------------------------------------

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

Las distintas divisiones bajo cuya responsabilidad se encuentran los servicios prestados deberán contemplar la seguridad desde el mismo momento en que se concibe un nuevo sistema o servicio, aplicando para estos y para los ya existentes, las medidas de seguridad prescritas por el Esquema Nacional de Seguridad para garantizar la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad de los servicios y de la información.

Los requisitos de seguridad de los sistemas, las necesidades de formación de los usuarios, administradores y operadores y las necesidades de financiación deben ser identificados e incluidos en la planificación de los sistemas y en los pliegos de prescripciones utilizados para la realización de proyectos que involucren a las TIC.

Se deben articular mecanismos de prevención, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad.

En cuanto a la prevención, se debe evitar que los servicios y la información resulten afectados por un incidente de seguridad. Para ello, la APV implementará las medidas de seguridad establecidas en el Anexo II del ENS, así como medidas adicionales que pudieran ser identificadas en el proceso de análisis de riesgos.

En cuanto a la reacción, se establecerán mecanismos de detección, comunicación y gestión de incidentes de seguridad, de forma que cualquier incidente pueda ser tratado en el menor plazo posible. Siempre que sea posible, se detectarán de forma automática los incidentes de seguridad, utilizando elementos de monitorización de los servicios o de detección de anomalías y poniendo en marcha los procedimientos de respuesta al incidente en el menor plazo posible. Para los incidentes detectados por los usuarios, ya sean internos o externos, se establecerán los pertinentes canales de comunicación de incidentes.

En cuanto a la recuperación, para aquellos servicios que se consideren críticos, en base a la valoración que de los mismos realicen sus responsables, se deberán desarrollar planes que permitan la continuidad de dichos servicios en el caso de que, a raíz de un incidente de seguridad, quedaran indisponibles.

6. Alcance

Esta Política de Seguridad es de aplicación a todos los servicios prestados por la APV que se apoyen en las Tecnologías de la Información y las Comunicaciones, así como a todo el personal, sin excepciones.

7. Organización de la Seguridad de la Información

La seguridad en la APV está soportada sobre los siguientes roles:

- Estructura de especificación, que es la que se encarga de establecer los requisitos de seguridad asociados a los servicios prestados.
- Estructura de supervisión, que es la que se encarga de verificar el cumplimiento de los requisitos de seguridad y el alineamiento continuo con los objetivos de la organización.
- Estructura de operación, que se encarga de implantar las medidas de seguridad identificadas.

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

7.1 Estructura de especificación

Esta estructura es la encargada de determinar los requisitos de seguridad que serán de aplicación a los servicios prestados por la APV y a garantizar el cumplimiento normativo asociado que le es de aplicación, en concreto el Real Decreto 3/2010 de 8 de enero por el que se regula el Esquema Nacional de Seguridad.

Se describen a continuación las funciones y responsabilidades de los roles asociados a la especificación.

7.1.1 Responsable de la Información

Es el responsable último de la protección de la información, garantizando su disponibilidad, confidencialidad e integridad.

Tiene la potestad de establecer los requisitos de seguridad de la información, en el sentido de asignarle a la misma una valoración que determinará el nivel de protección que requiere. El establecimiento de requisitos podrá realizarlo a propuesta del Responsable de Seguridad de la Información y contando con la opinión del Responsable del Sistema.

Este rol podrá recaer en una o varias personas, e incluso en un órgano colegiado, pudiendo coincidir con el Responsable del Servicio.

7.1.2 Responsable del Servicio

Es el responsable de determinar los niveles de seguridad que requieren los servicios prestados, que establecerán las medidas de protección necesarias y su intensidad.

El establecimiento de requisitos podrá realizarlo a propuesta del Responsable de Seguridad de la Información y contando con la opinión del Responsable del Sistema. Los requisitos del servicio deben tener en cuenta los requisitos de la información que manejan.

Este rol podrá recaer en una o varias personas, e incluso en un órgano colegiado, pudiendo coincidir con el Responsable de la Información.

7.1.3 Responsable del Tratamiento

El Responsable del Tratamiento es la persona física o jurídica sobre la que recaen las funciones genéricas recogidas en la normativa de protección de datos aplicable y vigente en cuanto a responsabilidad última de los tratamientos de datos personales que se lleven a cabo.

En general, esta figura determina los fines y los medios relacionados con el tratamiento de los datos personales.

Sus funciones son las siguientes:

- Garantizar el cumplimiento de principios relativos al tratamiento recogidos en la normativa vigente en materia de protección de datos personales.
- Garantizar el cumplimiento de las normativas existentes en la Autoridad Portuaria de Vigo en materia de protección de datos personales.

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

- Garantizar el mantenimiento adecuado, y conforme a la legislación vigente, del Registro de Actividades de Tratamiento.
- Garantizar el cumplimiento del deber de información al interesado recogido en la normativa vigente en materia de protección de datos personales.
- Establecer los mecanismos necesarios para recibir, gestionar y resolver solicitudes de ejercicio de derechos por parte de los interesados.
- Evaluar el riesgo para los derechos y libertades de los afectados en las brechas de seguridad y la posible notificación a las autoridades de control y a los afectados.
- Determinar las medidas técnicas y organizativas apropiadas que se debe aplicar a fin de garantizar y acreditar que el tratamiento es conforme con la normativa vigente de protección de datos personales.
- Actuar como punto de contacto con las autoridades de control, conjuntamente con el Delegado de Protección de Datos.
- Implantar y seguir los programas de formación y sensibilización del personal de la Autoridad Portuaria de Vigo en materia de protección de datos personales.

7.2 Estructura de supervisión

La estructura de supervisión de la seguridad de la información se encarga de verificar la correcta implantación y operación de los requisitos de seguridad que se hayan establecido, de cara a mantener la alineación con los objetivos y de cumplir con las normas y legislación aplicable.

En la supervisión global de todas las actividades relativas a la seguridad de la información se encuentra el Responsable de Seguridad de la Información.

En la supervisión global de las actividades relativas a la seguridad física se encuentra el Responsable de Seguridad Física.

Para la coordinación global e integral de la seguridad de la información se encuentra el Comité de Seguridad de la Información.

Las funciones y responsabilidades de cada una de las figuras se describen a continuación:

7.2.1 Responsable de Seguridad de la Información

Es responsable de la definición, coordinación, difusión y verificación de los requisitos de seguridad de la información en la Organización.

Este Responsable forma parte del Comité de Seguridad de la Información y, por tanto, es el encargado de elevar a dicho Comité los asuntos de interés relacionados con la seguridad de la información.

Sus responsabilidades comprenden:

- Coordinar y controlar las medidas de seguridad de la información y de protección de datos de la Organización.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de las normas y procedimientos establecidos.
- Conseguir que se elabore el presupuesto anual de seguridad TI de la Organización.

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

- Definir un modelo de gestión de la seguridad alineado con la estrategia de la Organización en materia de seguridad. A este modelo de gestión se le llamará SGSI, independientemente de que esté basado en las normas internacionales que recomiendan cómo hacerlo, o se trate de un modelo diferente.
- Supervisar la implantación práctica de la estrategia de seguridad de la información de la Organización.
- Supervisar las situaciones excepcionales (o incidentes) de ciberseguridad producidas en la Organización.
- Promover la realización de análisis de riesgos de seguridad de la información de forma periódica.
- Solicitar a la División de Recursos Humanos la realización de programas de formación y sensibilización en materia de seguridad de la información.
- Analizar los indicadores de seguridad para medir la eficacia y eficiencia de las medidas implantadas.
- Analizar los incidentes de seguridad de la información reflejados en los registros de estos y verificar que se han establecido los planes para su resolución.
- Mantener actualizada la documentación asociada a la gestión de la seguridad de la información: normativas, procedimientos y registros.
- Autorizar por escrito la ejecución de procedimientos de recuperación de datos en los casos en que se requiera.
- Colaborar con las Auditorías externas/internas en materia de seguridad de la información, revisarlas y encargar a los responsables de los sistemas la implantación de las correcciones que se deriven.

7.2.2 Responsable de Seguridad Física

Es responsable de la definición, coordinación, difusión y verificación de los requisitos de seguridad física en la Organización que tengan relación con las tecnologías de la información.

Este Responsable forma parte del Comité de Seguridad de la Información y, por tanto, es el encargado de elevar a dicho Comité los asuntos de interés relacionados con la seguridad física de los locales y las infraestructuras relacionadas con las tecnologías de la información.

Sus responsabilidades comprenden:

- Identificación de necesidades de seguridad física.
- Conseguir la elaboración de un presupuesto anual de inversiones y actuaciones en seguridad física.
- Supervisar la instalación y el mantenimiento posterior de los elementos y servicios destinados a la seguridad física.
- Analizar los incidentes de seguridad física que se puedan haber producido y establecer actuaciones para dar respuesta a los mismos.
- Participar en el Comité de Seguridad de la Información.

7.2.3 Delegado de Protección de Datos

El Delegado de Protección de Datos es la figura que actúa como asesor, supervisor e interlocutor del Responsable del Tratamiento en el ámbito de las competencias marcadas por la normativa en materia de protección de datos vigente.

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

Sus funciones son:

- Informar y asesorar a la Autoridad Portuaria de Vigo y a todos los empleados que se ocupen del tratamiento de datos personales, de las obligaciones que se deriven del Reglamento General de Protección de Datos y de otras disposiciones relacionadas con la protección de datos.
- Supervisar el cumplimiento del Reglamento General de Protección de Datos en la Autoridad Portuaria de Vigo.
- Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la Autoridad de Control.
- Actuar como punto de contacto de la Autoridad de Control conjuntamente con el Responsable del Tratamiento.

Además, asesorará al Responsable del Tratamiento o, en general, a aquella figura que lo necesite, en las siguientes áreas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de la compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación entre la Autoridad Portuaria de Vigo y los encargados del tratamiento.

7.2.4 Comité de Seguridad de la Información

La misión del Comité de Seguridad de la Información es la coordinación general de las actividades que tienen relación con la seguridad integral.

Un objetivo fundamental del Comité de Seguridad de la Información es la puesta en común de aspectos importantes de la seguridad entre todos los responsables. Con ello se evitará que actividades referentes a la seguridad, que puedan afectar a varias o todas las divisiones de la organización, queden sin el suficiente conocimiento por parte de sus responsables, o sin el suficiente apoyo o compromiso, perjudicando la eficacia.

Las funciones del Comité de Seguridad de la Información son:

- Informar regularmente del estado de la seguridad a la Dirección
- Revisar regularmente la Política de Seguridad y proponer cambios, si procede.

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

- Revisar las normativas internas de seguridad que se puedan derivar de la Política de Seguridad y proponerlas para su aprobación.
- Elaborar y proponer los requisitos de formación para el personal clave que maneja información y sistemas.
- Asumir el papel de dueño de los riesgos de seguridad de la información (quien tiene la potestad para aceptar los riesgos residuales sobre los activos), aprobando las apreciaciones de riesgos realizadas y aceptando el riesgo residual resultante, en su caso.
- Aprobar los planes de tratamiento de riesgos que surjan a raíz de las apreciaciones de riesgos realizadas.
- Seguir el desarrollo de los planes de acción aprobados.
- Coordinar las actuaciones en materia de seguridad que se puedan estar realizando en diferentes divisiones de la Organización con objeto de evitar esfuerzos duplicados o desalineados con la Política de Seguridad
- Analizar incidentes de seguridad significativos. Decidir qué hacer a raíz de ellos. Algunos pueden conllevar una actuación con gasto, en cuyo caso se propondría para su aprobación.
- Analizar información de indicadores de seguridad que pudiera haber definidos. Tomar decisiones en caso de desviación respecto a los umbrales establecidos.
- Proponer soluciones de seguridad que deban tener un presupuesto aprobado.

Serán miembros fijos del Comité de Seguridad de la Información:

- La Directora de la Autoridad Portuaria de Vigo
- El Jefe de Departamento de Tecnologías
- El Responsable de Seguridad de la Información
- Los Responsables de áreas con uso de las TIC
- El Responsable de Seguridad Física

Adicionalmente, podrán asistir al Comité de Seguridad de la Información los responsables de las materias específicas a tratar en las reuniones, que podrán ser invitados en función del contenido de la agenda.

7.3 Estructura de Operación

La estructura de operación de la seguridad debe asumir la administración operativa de la seguridad de los sistemas de información, implantando en dichos sistemas las medidas necesarias para satisfacer los requisitos de seguridad establecidos por la estructura de especificación.

Se describen a continuación las funciones y responsabilidades de las figuras asociadas a la estructura de operación.

7.3.1 Responsable de los Sistemas de Información

Sus funciones y responsabilidades son:

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

- Definir, en coordinación con el Responsable de Seguridad de la Información, las especificaciones funcionales de seguridad de los Sistemas de Información de la Organización.
- Garantizar que en el diseño de sistemas de información y redes de comunicaciones se contemplen desde el principio los aspectos necesarios de seguridad de la información en cuanto a disponibilidad, integridad, confidencialidad, autenticación, control de acceso, auditoría y registro.
- Revisar que la configuración de seguridad tras la instalación de un sistema nuevo es la adecuada (perfil inicial de seguridad. Bastionado).
- Revisar que la configuración de seguridad tras los cambios en un sistema sigue siendo la adecuada.
- Verificar el funcionamiento de mecanismos de Control de Acceso que eviten que un usuario acceda a datos o recursos con derechos distintos de los autorizados, sin que en ningún caso se puedan desactivar.
- Seguir los foros de vulnerabilidades y elaboración del calendario de aplicación de parches para los sistemas de información, en función de los que surjan y el impacto que tengan en la seguridad (los parches mismos los aplicarán los administradores de sistemas).
- Implantar las medidas de seguridad que resulten de los planes de tratamiento de riesgos o planes de acciones correctivas a raíz de las auditorías de seguridad de la información.
- Proporcionar datos para la alimentación de indicadores de seguridad de la información.
- Supervisar los procedimientos de copia de seguridad.
- Realizar auditorías técnicas periódicas de la infraestructura de tecnologías de la información, sistemas y aplicaciones.

7.4 Designación de roles de las estructuras de seguridad

Se establece que el Comité de Seguridad de la Información es el órgano con potestad para designar y modificar la designación de roles del gobierno de la seguridad de la información.

Las designaciones o modificaciones se recogerán en el acta de la sesión del Comité de Seguridad de la Información correspondiente, que constituirá el documento justificativo de tales nombramientos.

7.5 Mecanismos de coordinación y de resolución de conflictos

La coordinación entre los diferentes roles participantes de las actividades de seguridad así como la resolución de conflictos que pudieran surgir entre ellos se llevará a cabo en el seno del Comité de Seguridad de la Información.

8. Obligaciones del Personal

Todo el personal de la APV que tenga algún tipo de relación con el uso, la gestión, mantenimiento y explotación de la información y de los servicios prestados por la APV tienen la obligación de conocer la Política de Seguridad de la Información y cumplirla. El Comité de Seguridad de la Información dispondrá los medios para que esta Política llegue a los afectados.

Así mismo, el personal deberá asistir a las sesiones de concienciación y formación en materia de seguridad para las que sea designado como asistente.

<p>CLASIF: USO INTERNO</p>	<p>Pag 17 de 20</p>	<p>APV STIC-POL-1 Política de Seguridad de la Información v1.0.docx</p>
-----------------------------------	----------------------------	--------------------------------------------------------------------------------

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

9. Terceras Partes

Las terceras partes que estén relacionadas con la gestión, mantenimiento o explotación de los servicios prestados por la APV serán hechos partícipes de esta Política. Las terceras partes quedarán obligadas al cumplimiento de esta Política y a las normativas que se puedan derivar de ella.

Las terceras partes podrán desarrollar sus propios procedimientos operativos para satisfacer la Política.

Se deberán establecer procedimientos específicos de comunicación de incidencias para que los terceros afectados puedan comunicarlas.

El personal de las Terceras Partes deberá recibir sesiones de concienciación, tal como se exige para el personal propio.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte, el Responsable de Seguridad de la Información deberá realizar un informe del riesgo en que se incurre. Ese riesgo deberá ser aceptado por el Comité de Seguridad de la Información.

10. Formación y Concienciación

De manera sistemática se realizarán acciones de formación y concienciación en materia de seguridad de la información.

El objetivo de la acción formativa y de concienciación es doble:

- mantener informado al personal más directamente relacionado con el manejo de información y los sistemas que la tratan sobre los procedimientos existentes de seguridad, configuración segura de equipos, desarrollo seguro, gestión de incidentes de seguridad, riesgos, etc.
- concienciar al personal, en general, de la importancia de la seguridad y de los procedimientos básicos de manejo e intercambio de información.

El primer objetivo se asocia a Formación y el segundo a Concienciación.

Todo el personal deberá asistir a una sesión de concienciación en materia de seguridad de la información con la periodicidad que se determine por parte del Comité de Seguridad de la Información.

Se establecerá un plan de concienciación para impartir las anteriormente mencionadas sesiones.

Las personas con responsabilidad en el uso, la gestión, mantenimiento o explotación de los servicios soportados en las 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 como si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Las áreas responsables determinarán el formato de la acción de formación, así como sus contenidos.

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

11. Gestión de Riesgos

Los servicios e información bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.

Como metodología base para la realización de los análisis de riesgos se utilizará Magerit, siendo esta metodología la más recomendable para el sector público nacional.

El análisis se realizará:

- regularmente, una vez al año.
- cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- cuando ocurra un incidente de seguridad grave.
- cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

El Comité de Seguridad de la Información establecerá los niveles aceptables de riesgo y aprobará las actuaciones a llevar a cabo en caso de que se incurra en niveles de riesgo no aceptables.

12. Datos de carácter personal

La Autoridad Portuaria de Vigo 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 legislación vigente en materia de Protección de Datos Personales.

13. Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad de la Información se desarrollará mediante la elaboración de otras políticas o normativas de seguridad que aborden aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.

La documentación de políticas y normativas de seguridad, así como esta Política de Seguridad de la Información se encontrará a disposición de todo el personal de la organización que necesite conocerla y, en particular, el personal que utilice opere o administre los sistemas de información y comunicaciones, la información misma albergada en dichos sistemas o los servicios prestados por la Autoridad Portuaria de Vigo.

14. Compromiso de la Presidencia

La Presidencia de la Autoridad Portuaria de Vigo manifiesta su compromiso formal con el apoyo a los planes de seguridad que se deriven de la aplicación de esta Política. Dicho apoyo se concretará en:

- proporcionar los recursos necesarios, dentro de las posibilidades presupuestarias;

 <p>Puerto de Vigo Autoridad Portuaria de Vigo</p>	<p>Política de Seguridad de la Información</p>	<p>Id: STIC-POL-01</p>
		<p>Versión: V1.0 11.03.21</p>
<p>ESQUEMA NACIONAL DE SEGURIDAD</p>		

- asignar roles y responsabilidades a las personas asociadas a los planes de seguridad;
- destinar presupuesto, dentro de las posibilidades;
- apoyar la formación de los recursos humanos implicados en los planes de seguridad para que adquieran el nivel de concienciación y las competencias necesarias;
- garantizar el mantenimiento de la documentación asociada a los planes de seguridad;
- facilitar las comunicaciones con otras organizaciones en materia de seguridad de la información;
- promover la mejora continua.

El mencionado compromiso se manifiesta con la aprobación del presente documento.

15. Revisión de esta Política

La presente Política de Seguridad de la Información será revisada con carácter anual por el Comité de Seguridad de la Información.