Política PL-01:

Política Seguridad Información

METADATA

	Elaborado	*Revisado*	*Aprobado*
Nombre	*Diego Camacho*		
Cargo	*Consultor Seguridad*		
Fecha	*28/01/2021*		

Propietario	*Máximo Sanz*
Clasificación	*Público*

HISTORIAL DE CAMBIO

Versión	*Fecha*	*Autor*	*Descripción cambio*
0.1	*26/04/2021*	*Diego Camacho*	*Creación primera versión*

Tabla de contenido

1. Introducción

La Autoridad Portuaria de la Bahía de Algeciras (en adelante APBA) considera a la información como un activo clave en el desempeño de su misión y en la búsqueda de su visión. Por tanto, la seguridad de la información es considerada una cuestión crucial y estratégica para la organización. El objetivo global de la seguridad de la información es preservar la disponibilidad, integridad y confidencialidad de la información.

La presente Política de Seguridad de la Información establece la intención y dirección de la APBA en relación con la seguridad de la información. La intención se explicita en los objetivos de seguridad recogidos en la presente política. La dirección se concreta con el alineamiento constante de la presente política con la dirección estratégica de la APBA.

La Alta Dirección de la APBA está comprometida a hacer todos los esfuerzos para cumplir con todos los requisitos de seguridad de la información que apliquen a la APBA. En este sentido y para asegurar una gestión sistemática de la seguridad de la información, la Alta Dirección de la APBA ha establecido un sistema de gestión de la seguridad de la información. La Alta Dirección de la APBA está comprometida a mejorar de forma continuada y mantenida en el tiempo el sistema de gestión de la seguridad de la información.

2. Ámbito Aplicación

La presente Política de Seguridad de la Información, así como otras políticas, normas, procesos y procedimientos derivados de ella, aplican a la información en cualquiera de sus estados y a los sistemas de información y comunicaciones que la APBA utiliza.

La Política de Seguridad de la Información es aplicable con carácter obligatorio a todo el personal de la organización, así como a las entidades colaboradoras que hagan uso de la información de la APBA o de los sistemas que la almacenan, procesan o transmiten.

3. Misión y Objetivos

La misión de la APBA es "*liderar una oferta portuaria y logística competitiva y sostenible, generadora de valor añadido, en estrecha colaboración con los clientes y en beneficio de la economía y empleo regionales*".

Los objetivos de la APBA dentro de su Plan Estratégico 2020 son:

- Mantener el liderazgo como puerto *hub* de contenedores del Mediterráneo occidental.
- Ser nodo logístico internacional del tráfico de graneles líquidos y *bunkering*.
- Afianzar la condición de puente marítimo de conexión logística con el continente africano.
- Desarrollo como centro de servicios al tráfico marítimo.

- Integrar al Puerto de Bahía de Algeciras en las cadenas de suministro y distribución internacionales consolidándose como la puerta sur de Europa.
- Mantener y mejorar la calidad y eficiencia de los servicios portuarios asociados a los tráficos de naturaleza industrial.
- Mantener un desarrollo sostenible con un uso limitado de los recursos, promoviendo productos y procesos con un impacto ambiental reducido.
- La optimización de la gestión y la mejora continua de los servicios.

4. Marco Normativo

La APBA gestiona los puertos Bahía de Algeciras y Tarifa. Es un organismo público que depende del Ministerio de Fomento, con personalidad jurídica y patrimonio propios, con plena capacidad de obra. La APBA se rige por el texto refundido de la Ley de Puertos del Estado y de la Marina Mercante aprobado por el Real Decreto Legislativo 2/2011, de 5 de septiembre.

El marco normativo para esta Política de Seguridad de la Información emana de las directivas de la Unión Europea y la Legislación Española relativas a protección de instalaciones de interés cuando sean de aplicación a las instalaciones y servicios que gestiona la APBA.

También forman parte del marco normativo las normas que sean de aplicación al uso de las herramientas de administración electrónica en la APBA, las que se deriven de las anteriores y las que se publiquen en la sede electrónica dentro del ámbito de la Política de Seguridad de la Información.

En el Anexo I de esta política se detalla el marco legal y regulatorio dentro del cual la APBA lleva a cabo sus actividades.

5. Organización Seguridad

5.1. Comités: Comité Consultivo de Protección Portuaria

El **Comité Consultivo de Protección Portuaria** se responsabiliza de alinear todas las actividades de la APBA en materia de seguridad, incluyendo la seguridad de la información, la seguridad física y la protección marítima. Está presidido por el Subdirector General de Explotación de la APBA y en él participan los máximos responsables de los diferentes departamentos. La definición completa de sus funciones y miembros se establece en el Plan de Seguridad del Operador (PSO) de la APBA. En lo relativo a la seguridad de la información, forman parte del Comité Consultivo de Protección Portuaria:

- Jefe del Área de Desarrollo Tecnológico (ADT).
- Responsable de Seguridad de la Información.

El Comité Consultivo de Protección Portuaria tiene, **en relación con la seguridad de la información**, las siguientes responsabilidades:

- Revisar y aprobar la presente Política de Seguridad de la Información conforme a los intervalos temporales que se determinen.
- Informar regularmente del estado de la seguridad de la información a la Dirección.

El Comité Consultivo de Protección Portuaria asume los roles de Responsable de Información y Responsable del Servicio cuyas responsabilidades se detallan más adelante en esta política.

5.2. Comités: Comité de Seguridad de la Información

El Comité de Seguridad de la Información depende jerárquicamente del Comité Consultivo de Protección Portuaria y tiene como ámbito de responsabilidad la apropiada gestión de la seguridad de la información.

El Comité de Seguridad de la Información tiene las siguientes responsabilidades:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos en materia de seguridad de la información.
- Informar regularmente del estado de la seguridad de la información al Comité Consultivo de Protección Portuaria.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información y someterla a aprobación por parte del Comité Consultivo de Protección Portuaria.
- Desarrollar, revisar y mantener la normativa de seguridad conforme a los intervalos temporales que se determine. Informar de la normativa de seguridad y de sus sucesivos cambios al Comité Consultivo de Protección Portuaria.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. 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.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir

La composición del Comité de Seguridad de la Información es la siguiente:

- Jefe del Área de Desarrollo Tecnológico (ADT).
- Responsable de Seguridad de la Información.
- Responsable del Sistema

Adicionalmente, se podrá invitar a otros responsables de la APBA de manera ad hoc cuando se vayan a tratar cuestiones de seguridad de la información que afectan o sean de especial interés de otras áreas de la APBA (por ejemplo, recursos humanos, protección de datos, etc.)

En el registro RG.PL-01.02 se recogen el resto de los términos de referencia del Comité de Seguridad de la Información.

5.3. Roles: funciones y responsabilidades

5.3.1. Responsable Información

Las responsabilidades del **Responsable de la Información** son las siguientes:

- Establecer los requisitos de la información en materia de seguridad. Es decir, determinar los niveles de seguridad de la información.
- La responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.

5.3.2. Responsable Servicio

Las responsabilidades del **Responsable del Servicio** son las siguientes:

- Establecer los requisitos del servicio en materia de seguridad. Es decir, determinar los niveles de seguridad del servicio. La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja.

5.3.3. Responsable Seguridad Información

Las responsabilidades del **Responsable de la Seguridad de la Información** son las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información, de acuerdo a lo establecido en la presente Política de Seguridad de la Información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Formar parte del Comité Consultivo de Protección Portuaria, asesorando en materia de seguridad de la información.
- Ejecutar directamente o bien delegar y supervisar la ejecución de las decisiones tomadas por el Comité.
- Elaborar, actualizar y divulgar la normativa de seguridad de la información aprobada por el Comité Consultivo de Protección Portuaria.
- Aprobar los procedimientos de seguridad elaborados por la ADT.

5.3.4. Responsable Sistema

Las responsabilidades del **Responsable del Sistema** son:

- Desarrollar, operar y mantener el sistema durante todo su ciclo de vida, incluyendo definición de especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del sistema 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.
- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada de forma previa con al menos otro miembro del Comité de Seguridad de la Información.

5.3.5. Administrador Seguridad

Si la complejidad del sistema lo requiere, podrá designarse uno o varios administradores de la seguridad del sistema, que dependerán del Responsable del Sistema. Las responsabilidades del **Administrador de Seguridad** son las siguientes (en caso de no designarse administradores de seguridad, estas responsabilidades recaen directamente sobre el Responsable del Sistema):

- La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema.
- La gestión de 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.
- La aplicación de los Procedimientos Operativos de Seguridad.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que se aplican los procedimientos aprobados para manejar el sistema.
- 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 Seguridad y al Responsable del Sistema 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.

5.3.6. Personal y terceros

Las responsabilidades del **personal de la APBA así como de cualquier tercera parte operando bajo la autoridad de la misma** en relación con la seguridad de la información son**:**

- Conocer y cumplir con las políticas de la organización que le atañen.
- Reportar cualquier actividad anómala sin dilación.
- Utilizar los activos de la organización de forma adecuada y conforme a las políticas de la organización.

5.4. Mecanismos Coordinación

El Comité Consultivo de Protección Portuaria da instrucciones al Responsable de Seguridad de la Información, que a su vez se encarga de supervisar que sean ejecutadas por el Responsable del Sistema, que a su vez supervisa a los administradores y operadores del sistema a su cargo.

De acuerdo con el principio de jerarquía que rige en las administraciones públicas españolas, en caso de conflicto este deberá ser resuelto por el superior jerárquico.

5.5. Procedimiento Designación

El Responsable de Información será designado por la Dirección y su nombramiento aprobado formalmente por el Presidente de la APBA.

El Responsable de Servicio será designado por la Dirección y su nombramiento aprobado formalmente por el Presidente de la APBA.

El Responsable de Seguridad será designado por la Dirección y su nombramiento aprobado formalmente por el Presidente de la APBA.

El Responsable del Sistema será designado por la Dirección y su nombramiento aprobado formalmente por el Presidente de la APBA.

El resto de los roles serán designados por la Dirección a propuesta del responsable del área en cuestión. En este sentido, se tendrán en cuenta el principio de separación de responsabilidades y se evitarán los potenciales conflictos de intereses.

Los individuos designados figurarán en el registro pertinente de la información documentada del sistema de gestión de la seguridad de la información.

6. Gestión Información Documentada

La información documentada es un importante soporte para el Sistema de Gestión de Seguridad de la Información (SGSI) y para una gestión sistemática de la seguridad de la información. En este sentido, la APBA ha establecido la norma ***NS-10 Gestión información documentada*** donde se establecen los requisitos y expectativas que APBA tiene en relación con la gestión de la información documentada en el ámbito de la seguridad de la información.

7. Aprobación

Esta política ha sido elaborada por el Responsable de Seguridad, revisada y aprobada por el Comité Consultivo de Protección Portuaria y por el Presidente de la APBA con fecha dd/ mm / aaaa.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

Firmado:

nombre y apellidos
Presidente de la Autoridad Portuaria de la Bahía de Algeciras

8. Registros y archivo

Identificación	*Registro*	*Responsable*	*Tipo Archivo*	*Retención*
RG.PL-01.01	Roles y Miembros	Responsable Seguridad	Electrónico	3 años
RG.PL-01.02	Términos referencia Comité Seg. Inf.	Responsable Seguridad	Electrónico	3 años

9. Anexo I

- Directiva 2008/114/CE del Consejo, sobre Identificación y Designación de las Infraestructuras Críticas Europeas y la Evaluación de la Necesidad de Mejorar su Protección.
- 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
- DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 3/2010, de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, 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.