Política PO-04:

Política Seguridad Información

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. Principios, Objetivos y Misión

Los principios de la seguridad de la información por los que se rige la APBA son:

1. **Confidencialidad**: Este principio se refiere a la protección de la información sensible para evitar su acceso no autorizado. Se logra mediante el uso de técnicas como el cifrado de datos y el control de acceso.
2. **Integridad**: Garantizar la integridad de la información implica protegerla contra la modificación no autorizada. Esto se logra mediante el uso de controles que detectan y previenen cambios no autorizados en los datos, como el uso de firmas digitales, el control de versiones de archivos y los sistemas de detección de cambios no autorizados.

3. **Disponibilidad**: La disponibilidad se refiere a garantizar que la información esté disponible y accesible cuando sea necesario. Esto implica la prevención de interrupciones mediante estrategias de respaldo de datos, redundancia de servidores, sistemas de recuperación de desastres y monitoreo constante.
4. **Autenticidad**: Este principio se refiere a garantizar que es quien dice ser o bien que garantiza la de la que proceden los datos.
5. **Trazabilidad**: Referido a garantizar que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Así como los mencionados en los artículos 5 y siguientes del Esquema Nacional de Seguridad:

- Seguridad como proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua.
- Reevaluación periódica.
- Diferenciación de responsabilidades.
- La seguridad como un proceso integral.
- Gestión de la seguridad basada en los riesgos.
- Prevención, detección, respuesta y conservación.
- Existencia de líneas de defensa.
- Vigilancia continua y reevaluación periódica.
- Diferenciación de responsabilidades.

Para la defensa de estos principios, se identifican los siguientes objetivos de seguridad dentro de la APBA:

1. Garantizar la confidencialidad, integridad y disponibilidad de la información que posea la APBA.
2. Proteger los activos críticos de la organización contra amenazas internas y externas.
3. Analizar y gestionar los riesgos inherentes en las diferentes actividades portuarias y en los sistemas de la información que las mantienen.
4. Garantizar el cumplimiento de leyes, regulaciones y estándares relacionados con la seguridad de la información.
5. Establecer procedimientos para la rápida y eficaz respuesta a incidentes de seguridad que puedan afectar a la organización.
6. Implantar planes para la recuperación de los sistemas y servicios después de un incidente, para asegurar la continuidad del negocio, garantizando la recuperación y resiliencia de la organización.

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 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.

Toda la normativa utilizada para la redacción de esta política, así como la que se encuentre en vigor en el momento de la consulta, está publicada en el "RE-04.01 Listado de Documentación Externa Aplicable".

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, pudiendo delegar ambos roles en las personas responsables de área que corresponda en cada servicio funcional, 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 “RE-05.01 Listado roles” 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.

Estos cargos serán revisados cada dos años o en el caso de que el cargo queda vacante.

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 PG-04. Documentación del SGS 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. Datos Personales

La APBA trata datos de carácter personal. El Registro de Actividades de Tratamiento, publicado en la web de la APBA, recoge los tratamientos afectados y los responsables correspondientes. Todos los sistemas de información de se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Registro de Actividades de Tratamiento.