MINISTERIO
DE TRANSPORTES
Y MOVILIDAD SOSTENIBLE

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Autoridad Portuaria de Bahía de Cádiz

Código:	POL-ENS-01
Fecha:	05/12/2025
Versión:	5.0
Clasificación:	USO PÚBLICO

HOJA DE ESTADO DEL DOCUMENTO

Versión	Fecha	Preparado	Cambios
Versión 1.0	18/06/2017	División TIC APBC	Versión inicial
Versión 2.0	01/04/2019	División TIC APBC	Actualización del documento
Versión 3.0	20/11/2023	BABEL / División TIC APBC	Actualización por adecuación al Esquema Nacional de Seguridad (ENS)
Versión 4.0	15/05/2025	OFICINA TÉCNICA S.I - GMV	Actualización por Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
Versión 5.0	05/12/2025	OFICINA TÉCNICA S.I - GMV	Actualización del documento

Revisado por:	Revisado por:	Aprobado por:
Responsable de Seguridad de la Información	Comité de Seguridad de la Información	Consejo de Administración
Fecha: 21/01/2026	Fecha: 10/02/2026	Fecha: Marzo 2026

ÍNDICE

1. RESUMEN EJECUTIVO 4
2. INTRODUCCIÓN 4
3. ALCANCE 5
4. MISIÓN DE LA ORGANIZACIÓN 6
5. MARCO LEGAL Y REGULATORIO 6
6. ORGANIZACIÓN DE LA SEGURIDAD 7
6.1. ROLES: FUNCIONES Y RESPONSABILIDADES 7
6.2. COMITÉ: FUNCIONES Y RESPONSABILIDADES 7
6.3. PROCEDIMIENTO DE DESIGNACIÓN 7
6.4. ATRIBUCIONES Y MECANISMOS DE RESOLUCIÓN DE CONFLICTOS 8
7. DATOS DE CARÁCTER PERSONAL 8
8. GESTIÓN DE RIESGOS 8
9. AUDITORÍA 8
10. OBLIGACIONES DEL PERSONAL 9
11. TERCERAS PARTES 9
12. ESTRUCTURA DE LA DOCUMENTACIÓN 9
12.1. PRIMER NIVEL: POLÍTICA DE SEGURIDAD 10
12.2. SEGUNDO NIVEL: NORMATIVAS Y PROCEDIMIENTOS DE SEGURIDAD 10
12.3. TERCER NIVEL: PROCEDIMIENTOS TÉCNICOS DE SEGURIDAD 10
12.4. CUARTO NIVEL: INFORMES, REGISTROS Y EVIDENCIAS ELECTRÓNICAS 10
12.5. OTRA DOCUMENTACIÓN. 10
13. VALIDEZ DEL DOCUMENTO 10
14. ANEXO I: MARCO NORMATIVO 12
14.1. LEGISLACIÓN Y NORMATIVA APLICABLE 12
15. ANEXO II: ROLES: FUNCIONES Y RESPONSABILIDADES. 13
15.1. FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN 13
15.2. ROLES, FUNCIONES Y RESPONSABILIDADES 14
15.2.1. DIRECCIÓN DE LA APBC 14
15.2.2. RESPONSABLE DE LA INFORMACIÓN 14
15.2.3. RESPONSABLE DEL SERVICIO 14
15.2.4. RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN 15
15.2.5. RESPONSABLES DE LOS SISTEMAS 16
15.2.6. DELEGADO DE PROTECCIÓN DE DATOS 17
15.2.7. RESPONSABLE DE SEGURIDAD FÍSICA (PBIP) 18

1. RESUMEN EJECUTIVO

La Autoridad Portuaria de Bahía de Cádiz (APBC) reconoce que la información que gestiona y la infraestructura tecnológica sobre la que se sustenta son activos estratégicos esenciales para alcanzar sus objetivos institucionales, operativos y de servicio público.

En consecuencia, esta Política de Seguridad de la Información de la APBC (PSI-APBC) establece el marco que permite proteger dichos activos frente a amenazas que puedan comprometer su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, alineándose con el Esquema Nacional de Seguridad (ENS) regulado por el Real Decreto 311/2022, así como con la legislación vigente en materia de administración electrónica, protección de datos y relaciones interadministrativas, como la Ley 39/2015 y la Ley 40/2015.

Esta PSI-APBC también toma como referencia las guías CCN-STIC emitidas por el Centro Criptológico Nacional (CCN), y mantiene concordancia con las políticas de seguridad de Puertos del Estado (PdE) y el Ministerio de Transportes y Movilidad Sostenibles (MITMS).

La APBC asume la seguridad de la información como una responsabilidad compartida e integrada en la gestión de sus sistemas TIC (Tecnologías de Información y Comunicaciones) y servicios. Por ello, promueve una cultura de concienciación, un enfoque basado en riesgos, una mejora continua y una respuesta eficaz ante incidentes de seguridad.

2. INTRODUCCIÓN

La APBC depende de los sistemas TIC para alcanzar sus objetivos, ejercer sus competencias y prestar los servicios que tiene atribuidos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados, para alcanzar dicho fin, buscará regirse por el marco normativo establecido por el RD 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad (ENS).

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

Los sistemas TIC de la APBC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere que la APBC establezca una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos de la APBC apliquen las medidas mínimas de seguridad exigidas por el ENS, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

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

El objeto último de la seguridad de la información es garantizar que la APBC pueda cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información de forma segura y conforme al marco normativo vigente.

En este sentido, y en cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el ENS, la APBC establece la presente PSI-APBC, basada en una serie de objetivos estratégicos y principios fundamentales de actuación:

- Mantener unos niveles de seguridad, en términos de **confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad** de la información y de los activos de información, ajustados y coherentes con las necesidades de la Organización.

- Considerar la información y los sistemas que la soportan como activos estratégicos. Con ello, la Dirección de la APBC asume el compromiso de alcanzar los niveles de seguridad necesarios que garanticen los requisitos anteriormente citados en todos los procesos donde se procese, almacene o transmita información.
- Garantizar la **difusión** de esta PSI-APBC y del marco normativo que la soporta, fomentando entre el personal interno y externo una cultura de concienciación en seguridad de la información como parte inherente a sus funciones.
- Promover un enfoque de **mejora continua**, basado en la consecución de objetivos, la implantación de controles adecuados, su evaluación constante y la incorporación de las mejoras necesarias.
- Adoptar esta PSI-APBC como la herramienta clave para **estructurar, promover y asegurar el cumplimiento** de las medidas de Seguridad de la Información en todos los servicios de la APBC.
- Velar por la existencia de mecanismos adecuados que aseguren la continuidad de las actividades tecnológicas apoyadas en los sistemas de información, garantizando su recuperación en plazos aceptables.
- Reducir o mitigar la probabilidad de ocurrencia de los riesgos que afecten a los activos de información, procesos y servicios de la Organización.

A continuación, se describen los principios básicos que rigen la seguridad de la información en la APBC:

a) **Seguridad como un proceso integral**: La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema.

b) **Gestión de la seguridad basada en los riesgos**: El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

c) **Prevención, detección, respuesta y conservación**: La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta. De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

d) **Existencia de líneas de defensa**: El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

e) **Vigilancia continua**: Permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

f) **Diferenciación de responsabilidades**: En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

3. ALCANCE

Esta PSI-APBC se aplica a todos los sistemas TIC de la APBC y a todos los miembros de la Organización. Específicamente, se aplica a los sistemas TIC que dan soporte a los servicios/información del negocio, al ejercicio de derechos y cumplimiento de deberes por medios electrónicos, y a la interacción por medios electrónicos con los ciudadanos, la Comunidad Portuaria y la Administración Pública.

Esta PSI-APBC es aplicable con carácter obligatorio tanto al personal interno como a las empresas externas que colaboren con la Organización y que hagan uso de los sistemas de información de la APBC. Cualquier actuación que afecte a la seguridad de la información deberá ajustarse a las disposiciones aquí establecidas.

El Comité de Seguridad de la Información de la APBC (CSI-APBC) tiene la responsabilidad de facilitar los recursos necesarios para que este documento sea accesible para el personal implicado, y será publicada y distribuida acorde a lo requerido por el RD 311/2022, de 3 de mayo por el que se regula el ENS.

4. MISIÓN DE LA ORGANIZACIÓN

La misión de la APBC consiste en impulsar, en colaboración con la Comunidad Portuaria y la Ciudad, el desarrollo logístico, industrial y turístico en nuestra zona de influencia, a través de la oferta de una infraestructura, servicios y conexiones intermodales competitivas, a fin de contribuir sosteniblemente al desarrollo del tejido empresarial y productivo al que servimos.

Las competencias se recogen en el artículo 25 del 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 (TRLPMM), publicado en el BOE núm. 253, de 20 de octubre de 2011, siendo estas las siguientes:

- La prestación de los servicios generales, así como la gestión y control de los servicios portuarios para lograr que se desarrollen en condiciones óptimas de eficacia, economía, productividad y seguridad, sin perjuicio de la competencia de otros Organismos.
- La ordenación de la zona de servicio del puerto y de los usos portuarios, en coordinación con las Administraciones competentes en materia de ordenación del territorio y urbanismo.
- La planificación, proyecto, construcción, conservación y explotación de las obras y servicios del puerto, y el de las señales marítimas que tengan encomendadas, con sujeción a lo establecido en esta ley.
- La gestión del dominio público portuario y de señales marítimas que les sea adscrito.
- La optimización de la gestión económica y la rentabilización del patrimonio y de los recursos que tengan asignados.
- El fomento de las actividades industriales y comerciales relacionadas con el tráfico marítimo o portuario.
- La coordinación de las operaciones de los distintos modos de transporte en el espacio portuario.
- La ordenación y coordinación del tráfico portuario, tanto marítimo como terrestre.

5. MARCO LEGAL Y REGULATORIO

El presente apartado define las responsabilidades legales y regulatorias de la APBC en el manejo de la información, en concordancia con su naturaleza legal y los deberes derivados tanto de normativas nacionales como sectoriales. Además, incluye las obligaciones que asume frente a terceros, asegurando la transparencia y el cumplimiento de todos los acuerdos establecidos.

- **Normativa Nacional y Sectorial**: Se compromete a adherirse rigurosamente a todas las leyes y regulaciones aplicables que rigen la seguridad de la información. Esto incluye, pero no se limita a, leyes de protección de datos (RGPD), regulaciones de seguridad de la información (ENS, NIS2), y cualquier otra legislación específica del sector que impacte directamente en las operaciones de la APBC.
- **Obligaciones Contractuales con Terceros**: Reconocerá y cumplirá con las disposiciones establecidas en los acuerdos con socios comerciales, clientes y otros terceros que impliquen el manejo de datos e información confidencial. Estos acuerdos deben reflejar las expectativas y responsabilidades en relación con la seguridad y el tratamiento adecuado de la información.
- **Actualización y Cumplimiento:** Se establecerán procedimientos para la revisión periódica de esta política de seguridad de la información, con el fin de asegurar que permanezca actualizada con respecto a los cambios en las leyes y normativas pertinentes. Además, se implementarán medidas de cumplimiento para verificar que las prácticas de seguridad de la información de la APBC estén alineadas con estos requisitos legales y regulatorios.

El presente epígrafe busca garantizar que todas las actividades relacionadas con la información dentro de la APBC sean ejecutadas en conformidad con los requisitos legales y reglamentarios vigentes, minimizando así riesgos legales y fortaleciendo la confianza de todas las partes interesadas.

Lo citado anteriormente viene desarrollado y especificado para el conjunto de disposiciones legales y normas a las cuales está sujeta la APBC en materia de seguridad de la información viene recogido en el "ANEXO I: Marco Normativo".

6. ORGANIZACIÓN DE LA SEGURIDAD

La seguridad de los sistemas de información comprometerá a todos los miembros de la APBC, además por imperativo legal, la responsabilidad máxima del ENS y de la protección de datos se encuentra en el Presidente/a de la APBC.

Para garantizar el cumplimiento del ENS, la APBC ha establecido una Organización de la seguridad de la información, designando roles y responsabilidades de seguridad, y constituyendo un Comité de Seguridad de la información.

6.1. ROLES: FUNCIONES Y RESPONSABILIDADES

La ha designado los siguientes roles para velar por la consecución y mantenimiento de un adecuado nivel de Seguridad de la Información en la Organización.

- Responsables de los Servicios y de la Información
- Responsable de Seguridad de la Información
- Responsables de los Sistemas
- Coordinador de Continuidad y Gestión de Crisis.

Adicionalmente, la APBC ha constituido su CSI-APBC. Los roles, funciones y responsabilidades se detallan en la presente política en el ANEXO II: ROLES: FUNCIONES Y RESPONSABILIDADES.

Los roles de responsable de servicio y de la información serán asumidos por el CSI-APBC.

6.2. COMITÉ: FUNCIONES Y RESPONSABILIDADES

El CSI-APBC es el órgano que dentro de la APBC coordina al más alto nivel la Seguridad de la Información.

Dicho CSI-APBC estará constituido por los siguientes miembros:

- Presidente/a del CSI-APBC: **Director de la Entidad**
- Vicepresidente/a del CSI-APBC: **Responsable de Área**
- Secretario/a del CSI-APBC: **Responsable de Seguridad de la Información.**
- Vocales:
  - **Responsables de los Servicios y de la Información.**
  - **Responsables de los Sistemas**.
  - **Responsable de Seguridad de la Información.**
  - **Delegado de Protección de Datos**.
  - **Responsable de Seguridad Física (PBIP)**.
  - **Representante de Personal.**
  - **Coordinador de Continuidad y Gestión de Crisis.**
- Otros vocales (con voz, pero sin voto): Personal interno y/o externo de acuerdo con la orden del día

El CSI-APBC asumirá las funciones asignadas a los Responsables de la Información y los Responsables del Servicio.

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

Los roles, funciones y responsabilidades se detallan en la presente política en el ANEXO II: ROLES: FUNCIONES Y RESPONSABILIDADES.

6.3. PROCEDIMIENTO DE DESIGNACIÓN

La APBC designará formalmente mediante resolución de Dirección a los siguientes responsables: Responsable de Seguridad de la Información, Responsable(s) de la Información y de los Servicios, y Responsables de los Sistemas, Coordinador de Continuidad y Gestión de Crisis.

El CSI-APBC quedará formalmente constituido mediante la aprobación del documento de "Designación de Roles y Constitución del Comité de Seguridad".

6.4. ATRIBUCIONES Y MECANISMOS DE RESOLUCIÓN DE CONFLICTOS

Ante situaciones de conflicto entre las figuras que componen la estructura organizativa de seguridad de la información definida en esta PSI-APBC, lo resolverá el Responsable de Seguridad, y en su ausencia, la decisión recaerá sobre la persona de sustitución que él designe. En el caso de que el conflicto se produjese entre los miembros del CSI-APBC, éste se resolverá, por su Presidente. En caso de conflictos entre los responsables que componen la estructura organizativa de la Seguridad y los responsables definidos en la normativa de Protección de Datos de Carácter Personal, prevalecerá la decisión que presente un mayor nivel de exigencia respecto a la protección de los datos de carácter personal. Posibles modificaciones tanto en su estructura como composición deberán cumplir:

- Los cambios en la representación del CSI-APBC serán propuestos por su Presidente y ratificados por el Director de la APBC.
- Los cambios en los roles de la estructura organizativa serán propuestos y ratificados por el CSI-APBC.

7. DATOS DE CARÁCTER PERSONAL

En el desarrollo de sus funciones, la APBC maneja datos personales por lo que, en cumplimiento de la normativa vigente, dispondrá de las medidas necesarias para llevar un registro de Actividades de Tratamiento.

Así mismo, todos los sistemas de información de la APBC cumplirán con los niveles de seguridad establecidos por el ENS y el RGPD, asegurando así la protección de los datos personales identificados en el mencionado Registro de Actividades de Tratamiento (RAT).

8. GESTIÓN DE RIESGOS

En relación con todos los sistemas de información incluidos en el alcance de esta PSI-APBC, se debe realizar un análisis de riesgos que evalúe las amenazas y riesgos a los que están expuestos, incluyendo aquellos relacionados con la protección de datos personales.

Este análisis de riesgos será la base para determinar las medidas de seguridad que deben adoptarse, además de los mínimos establecidos por el ENS.

Este análisis se repetirá en las siguientes circunstancias:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada o los servicios prestados
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el CSI-APBC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados, esta debe ser revisada y aprobada por los correspondientes responsables de la información y servicios.

9. AUDITORÍA

De acuerdo con lo establecido en el ENS, los sistemas de información de la APBC se someterán a una auditoría en base a los siguientes periodos y criterios:

- Ordinaria: Periodo bienal.
- Extraordinaria: Siempre que se produzcan modificaciones sustanciales en el Sistema de Información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de la APBC están obligados a conocer y cumplir con esta PSI-APBC y su Normativa de Seguridad. Es responsabilidad del CSI-APBC proporcionar los medios necesarios para que esta información llegue a todos los empleados afectados.

La APBC promoverá la lectura y comprensión de las directrices generales de seguridad definidas en esta PSI-APBC, de manera que el personal actúe alineado con los principios y objetivos establecidos por la Organización.

Todos los miembros atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la APBC , en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

El incumplimiento de esta PSI-APBC y de su Normativa de Seguridad podrá conllevar medidas disciplinarias, que serán determinadas de acuerdo con la gravedad de la infracción y conforme a la normativa vigente, sin que por ello extinga las vías legales, tanto penales como administrativas.

11. TERCERAS PARTES

En las ocasiones en que la APBC preste servicios o maneje información de otros Organismos, se les informará sobre esta PSI-APBC. Además, se crearán canales de reporte y coordinación entre los respectivos Comités de Seguridad de la Información y se establecerán procedimientos conjuntos para la respuesta ante incidentes de seguridad.

Cuando la APBC reciba servicios de terceros o comparta información con terceros, se les informará de esta PSI-APBC, de su Normativa de Seguridad y de los Procedimientos de Seguridad aplicables a dichos servicios o información. Estos terceros deberán cumplir con las obligaciones establecidas en dicha normativa y podrán desarrollar sus propios procedimientos operativos para cumplirla. Se establecerán procedimientos específicos para el reporte y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta PSI-APBC.

Cuando algún aspecto de la PSI-APBC no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la Información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información/ servicios afectados antes de seguir adelante.

12. ESTRUCTURA DE LA DOCUMENTACIÓN

La documentación relativa a la Seguridad de la Información se clasificará en cuatro niveles, estructurados jerárquicamente de la siguiente manera:

- **Primer nivel:** Política Seguridad de la Información.
- **Segundo nivel:** Normativas y Procedimientos de Seguridad.
- **Tercer nivel:** Procedimientos Técnicos de Seguridad.
- **Cuarto nivel:** Registros y Evidencias Electrónicas.

Cada documento de un nivel inferior se basa y complementa la información de los niveles superiores para proporcionar una visión completa y detallada de las medidas y controles de seguridad implementados, no pudiendo negar o contradecir un documento de nivel superior.

12.1. PRIMER NIVEL: POLÍTICA DE SEGURIDAD

Es un documento de obligado cumplimiento por todo el personal, tanto interno como externo de la Organización. Este documento deberá estar debidamente formalizado y aprobado mediante resolución de por el Consejo de Administración de este Organismo Público.

Establece las bases y directrices generales sobre la seguridad de la información en la que estarán sustentados el resto de los documentos de niveles inferiores.

12.2. SEGUNDO NIVEL: NORMATIVAS Y PROCEDIMIENTOS DE SEGURIDAD

Las normativas y procedimientos de seguridad de este nivel son de obligado cumplimiento y se aplican según el ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de elaboración y/o aprobación de los documentos redactados en este nivel será competencia del Responsable de Seguridad de la Información bajo la supervisión del CSI-APBC, garantizando así la correcta alineación con la PSI-APBC y los requisitos legales y técnicos pertinentes.

12.3. TERCER NIVEL: PROCEDIMIENTOS TÉCNICOS DE SEGURIDAD

Los documentos técnicos destinados a resolver tareas críticas de seguridad, desarrollo, mantenimiento y/o explotación de los sistemas de información, buscan la mitigación de los riesgos de actuaciones inadecuadas.

La aprobación de dichos procedimientos técnicos corresponde a los Responsables de los Sistemas, supervisado por el Responsable de Seguridad de la Información. En caso de necesidad podrán ser elevados al CSI-APBC.

12.4. CUARTO NIVEL: INFORMES, REGISTROS Y EVIDENCIAS ELECTRÓNICAS

La documentación de este nivel recoge resultados y conclusiones de estudios o valoraciones, amenazas y vulnerabilidades de los sistemas de información y las evidencias electrónicas generadas durante las fases del ciclo de vida de los sistemas.

La responsabilidad de elaboración y/o aprobación recae en los Administradores de Seguridad de los Sistemas bajo la supervisión de los Responsables de los Sistemas.

12.5. OTRA DOCUMENTACIÓN.

Los procedimientos STIC, las normas STIC, las instrucciones técnicas STIC y las guías CCN-STIC, las normativas ISO/IEC, normativa NIS2, entre otros se pueden seguir en todo momento para complementar la documentación de seguridad.

13. VALIDEZ DEL DOCUMENTO

Este documento constituye la versión actualizada de la PSI-APBC de la APBC. Su validez se extiende desde la firma de esta, hasta la próxima revisión programada o hasta que circunstancias excepcionales requieran una actualización anticipada para responder a cambios significativos en el entorno legal, tecnológico o de seguridad. Teniendo en consideración lo siguiente:

- Deberá ser aprobado por la Alta dirección de la APBC
- Estará sujeta a una revisión anual regular.
- Deberá revisarse cuando se detecten cambios significativos en la APBC

La revisión anual de la PSI-APBC corresponde al CSI-APBC proponiendo en caso de que sea necesario mejoras de esta.

La efectiva gestión y cumplimiento de esta PSI-APBC son esenciales para proteger los activos de información de la entidad y garantizar la seguridad de nuestros sistemas y datos. Por lo tanto, es mandatorio que todos los empleados y partes interesadas comprendan su contenido y asuman las responsabilidades que les correspondan conforme a las directrices aquí establecidas.

14. ANEXO I: MARCO NORMATIVO

Este punto busca establecer las directrices para garantizar que la seguridad de la información en la Organización se administra de manera continuada y eficaz en el ámbito de los requisitos legales y normativas aplicables.

Para dar conformidad a lo anterior, el CSI-APBC es el responsable de supervisar y garantizar la ejecución efectiva de las revisiones periódicas de la PSI-APBC. Entre estas revisiones, se realizará la supervisión cada seis meses o siempre que se conozca de cambios significativos en la legislación o el entorno operativo que pueda afectar a la legislación aplicable.

El proceso de revisión consistirá en:

1. Evaluación de los cambios en el entorno legal y tecnológico.
2. Análisis de las recomendaciones y aportaciones realizadas por auditorías tanto internas como externas.
3. Ratificación de las modificaciones por el CSI-APBC.

A través de este enfoque proactivo, no solo se minimizan los riesgos legales, sino que también se refuerza la solidez de la PSI-APBC, garantizando estar siempre alineados con las normativa y legislación vigente.

14.1. LEGISLACIÓN Y NORMATIVA APLICABLE

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

Legislación General sobre la Administración Pública

- 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 (BOE: 20/10/2011).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (BOE: 02/10/2015).
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, artículo 3: principios de uso de medios electrónicos.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno.
- 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.

Legislación sobre Protección de Datos y Derechos Digitales

- Reglamento General de Protección de Datos (RGPD) (UE) 2016/679, aplicable desde el 25 de mayo de 2018 (DOUE: 04/05/2016).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE: 06/12/2018).
- Directiva 2002/58/CE, sobre la Privacidad y las Comunicaciones Electrónicas.

Normativa sobre Seguridad de la Información, Ciberseguridad y Administración Electrónica

- Real Decreto 411/2014, de 6 de junio, por el que se regulan cambios en el proceso de firma electrónica (BOE: 13/06/2014).
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. Real Decreto 931/2022, de 25 de octubre, por el que se regula el Esquema Nacional de Interoperabilidad.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) (BOE: 04/05/2022).Directiva (UE) 2022/2555, de 14 de diciembre, conocida como Directiva NIS2, aplicable desde el 16 de enero de 2023 (DOUE: 27/12/2022).
- Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (Reglamento eIDAS).

- 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 34/2002, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE). Norma internacional ISO/IEC 27001:2022.

Normativa Complementaria

- Real Decreto-ley 19/2020, de 26 de mayo, sobre medidas urgentes en administración digital y contratación pública (BOE: 27/05/2020).

Instrucciones Técnicas de Seguridad (ITS) del Esquema Nacional de Seguridad (ENS)

1. Informe del Estado de la Seguridad.
2. Guías CCN-STIC del CCN como referencia técnica para el desarrollo de la PSI-APBC.
3. Conformidad con el ENS. Auditoría de la Seguridad de los Sistemas de Información.
4. Notificación de Incidentes de Seguridad.

15. ANEXO II: ROLES: FUNCIONES Y RESPONSABILIDADES.

15.1. FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Son funciones típicas del CSI-APBC:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- 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 PSI-APBC para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la información.
- 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.
- Participar en la categorización de los sistemas y en el análisis de riesgos.
- Revisar y aprobar los análisis de riesgos de los sistemas de información y los planes de acciones para mitigarlos, así como dar seguimiento al cumplimiento de estos.
- 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.

- Asumir el rol central en la Gestión de Crisis y Continuidad del Negocio, liderando la coordinación de la respuesta ante incidentes y garantizando una actuación eficaz y alineada con los protocolos establecidos.
- Coordinación y supervisión al más alto nivel del cumplimiento de la normativa la vigente en materia de seguridad:
  - Reglamento General de Protección de Datos (RGPD) de la Unión Europea.
  - Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
  - Real Decreto 311/2022, de 3 de mayo, Esquema Nacional de Seguridad (ENS).

15.2. ROLES, FUNCIONES Y RESPONSABILIDADES

El presente documento pretende identificar unos claros responsables para velar por la consecución y mantenimiento de un adecuado nivel de Seguridad de la Información. Para ello se establecen los siguientes roles en la Organización relacionados con la Seguridad de la Información con las funciones y responsabilidades detalladas a continuación.

15.2.1. DIRECCIÓN DE LA APBC

- Para las entidades del Sector Público del ámbito de aplicación del ENS, el titular ostenta la máxima responsabilidad en el desarrollo de las competencias de la entidad, incluyendo las de seguridad de la información, de conformidad con lo dispuesto en la Ley 40/2015 y en el resto del ordenamiento jurídico.
- El Titular de la APBC, apoyado por los Responsables de Servicios y de la Información es el responsable de fijar los objetivos estratégicos, organizar adecuadamente sus elementos constituyentes, sus relaciones internas y externas, y dirigir su actividad, incluyendo la aprobación de la PSI-APBC del Organismo, así como, en su caso, la Política de Protección de Datos, facilitando los recursos adecuados para alcanzar los objetivos propuestos, velando por su cumplimiento.
- La figura de la Dirección de la entidad (personificada en su Titular) cobra una importancia capital: **de la Dirección depende el compromiso de la entidad con la seguridad y su adecuada implantación, gestión y mantenimiento.**

15.2.2. RESPONSABLE DE LA INFORMACIÓN

- El Responsable de la Información tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Determina los requisitos (de seguridad) de la información tratada según los parámetros del Anexo I del ENS. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de la información constituye asimismo una actividad indelegable.
- Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
- El Responsable de la Información es el propietario de los riesgos sobre la información.

Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta al Responsable de Seguridad la Información y conviene que escuche la opinión de los Responsables de los Sistemas.

15.2.3. RESPONSABLE DEL SERVICIO

- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.

- El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
- Valorará las consecuencias de un impacto negativo sobre la seguridad de los servicios, se efectuará atendiendo a su repercusión en la capacidad de la Organización para el logro de sus objetivos, la protección de sus activos, el cumplimento de sus obligaciones de servicio, el respeto de legalidad y derechos de los ciudadanos.
- Establece los requisitos de los servicios en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de los servicios.
- El Responsable del Servicio es el propietario de los riesgos sobre los servicios.

Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, podrá recabar una propuesta al Responsable de Seguridad la Información y conviene que escuche la opinión de los Responsables de los Sistemas.

La prestación de un servicio siempre debe atender a los requisitos de Seguridad de la Información que maneja, de forma que pueden heredarse los requisitos de seguridad de esta, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

15.2.4. RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN

Las dos funciones esenciales del Responsable de Seguridad la Información son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la PSI-APBC.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Adicionalmente, también deberá realizar las siguientes funciones:

- Elaborar y proponer para aprobación por la Organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciber incidentes que afecten a la Organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la Organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del RD-l 12/2018 y de su Reglamento de Desarrollo.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.
- En caso de ocurrencia de incidentes de Seguridad de la Información, analizará y propondrá salvaguardas que prevengan incidentes similares en un futuro.
- Convocará al CSI-APBC, recopilando la información pertinente.
- Velará por la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la PSI-APBC.
- Es el responsable de la supervisión de la eficacia de las medidas de seguridad establecidas para proteger la información y los servicios prestados por los sistemas de información.
- Asesorará a otros responsables en la determinación de las medidas de seguridad necesarias a partir de los requisitos de seguridad establecidos por el contexto interno y externo de la Organización.
- Promoverá la formación y concienciación en materia de Seguridad de la Información dentro de su ámbito de responsabilidad.

- Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría de los Sistema de Información.
- Realizará el Análisis de Riesgos.
- Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos.
- Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS.
- Participará en la elaboración y aprobación, en el marco del CSI-APBC, de las Normativas de Seguridad de la Información.
- Participará en la elaboración y aprobará los Procedimientos Operativos de Seguridad de la Información.
- Facilitará periódicamente al CSI-APBC un resumen de actuaciones en materia de seguridad, de incidentes relativos a Seguridad de la Información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).
- Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el CSI-APBC.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el CSI-APBC.
- Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el CSI-APBC y probados periódicamente por los Responsables de los Sistemas.
- Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

15.2.5. RESPONSABLES DE LOS SISTEMAS

Los Responsables de los Sistemas se encargan de la operación de los sistemas de información, atendiendo a las medidas de seguridad determinadas por el Responsable de Seguridad de la Información. Las funciones de los Responsables de los Sistemas serán las siguientes:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de Seguridad de la Información competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.
- Llevar a cabo las funciones del administrador de la seguridad del sistema cuando no se disponga de uno:
    - La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.
    - 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 de Información.
    - La gestión de las autorizaciones concedidas a los usuarios del sistema de información, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema de información se ajusta a lo autorizado.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.
    - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
    - Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
    - Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
    - Monitorizar el estado de seguridad del sistema de información proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema de información.
    - Informar al Responsable de Seguridad de la Información de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

15.2.6. DELEGADO DE PROTECCIÓN DE DATOS

El Delegado de Protección de Datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento. De manera excepcional, en aquellas organizaciones que, por su tamaño y recursos, no pudieran observar separación de roles, sería admisible la designación del delegado de protección de datos a la misma que ejerciese las funciones de Responsable de Seguridad de la Información, siempre que en la misma concurran los requisitos de formación y capacitación previstos por el RGPD. Las funciones del Delegado de Protección de Datos serán las siguientes:

- Supervisar el cumplimiento de lo dispuesto por el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, así como por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Supervisar el cumplimiento de lo dispuesto en el presente documento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.
- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento General de Protección de Datos y de la Ley Orgánica 3/2018.
- Mantenimiento del Registro de Tratamiento de Datos de Carácter Personal.
- Asesoramiento y supervisión en las siguientes áreas:
    - Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos
    - Cumplimiento del deber de información al interesado.
    - Identificación de las bases jurídicas de los tratamientos.
    - Valoración de 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 las 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 responsable-encargado.
    - Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la Organización y de las razones que justifiquen la transferencia.
    - Diseño e implantación de políticas de protección de datos.
    - Auditoría de protección de datos.
    - Establecimiento y gestión de los registros de actividades de tratamiento.
    - Análisis de riesgo de los tratamientos realizados.
    - Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
    - Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
    - Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
    - Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
    - Realización de evaluaciones de impacto sobre la protección de datos.

- Relaciones con las autoridades de supervisión. Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

15.2.7. RESPONSABLE DE SEGURIDAD FÍSICA (PBIP)

La APBC gestiona información clasificada conforme al Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (PBIP), normativa de obligado cumplimiento cuyo objetivo es garantizar la protección frente a amenazas deliberadas en el entorno marítimo-portuario.

El correspondiente Plan de Protección de la Instalación Portuaria (PPIP), de acceso restringido al personal autorizado, detalla los requisitos exigidos por el PBIP, así como los roles operativos necesarios para su aplicación. Entre ellos, destaca la figura del Oficial de Protección Portuaria (OPIP), cuya designación es obligatoria conforme al marco normativo vigente.

El OPIP asume funciones clave, entre las que se encuentran:

- Elaborar, implementar y mantener el PBIP.
- Evaluar riesgos y amenazas de tipo físico u operativas que puedan afectar a la instalación portuaria.
- Coordinar y supervisar medidas de protección, inspecciones y control de accesos a zonas restringidas.
- Dirigir simulacros, auditorías y revisiones del plan.
- Impulsar la formación del personal en materia de protección portuaria, conforme a los estándares del Código PBIP.

Dado que parte de estos requisitos tienen impacto sobre la seguridad de la información, especialmente en lo relativo al control de accesos, comunicaciones sensibles y gestión de incidentes, la APBC aplica medidas técnicas y organizativas en sus sistemas TIC alineadas tanto con el PBIP como, en lo que resulte aplicable, con el ENS. Esta coordinación permite abordar de forma integral las amenazas físicas y digitales, proteger activos críticos y garantizar la respuesta ante incidentes complejos.

En este contexto, el OPIP colabora con el órgano colegiado responsable de la seguridad de la información, con el fin de asegurar la coherencia entre las medidas de protección física, operativa y tecnológica implementadas en el ámbito portuario.

15.2.8. COORDINADOR DE CONTINUIDAD Y GESTIÓN DE CRISIS

El Coordinador de Continuidad y Gestión de Crisis será designado por el Presidente del Organismo Público, quien será el encargado de coordinar la respuesta institucional ante situaciones de alto impacto para asegurar la continuidad de la actividad. En caso de que un incidente de seguridad escale y se considere una crisis operativa, esta figura será la responsable de activar el Plan de Continuidad y Gestión de Crisis, conforme a los procedimientos establecidos en el marco de seguridad de la Organización.

Las funciones del Coordinador de Continuidad y Gestión de Crisis serán las siguientes:

- Activación del Plan de continuidad y Gestión de Crisis.
- Bajo el criterio del CSI-APBC, podrá solicitar diferentes perfiles según la naturaleza y nivel de crisis.
- Coordinación de las actividades de respuesta y recuperación.
- Informar a los órganos de dirección sobre el estado y la evolución de la crisis.
- Registro de la bitácora de actividad de la crisis.
- Elaboración del informe final de crisis en colaboración con el CSI-APBC y equipo participante.
- Cierre de la crisis.
- Coordinación del programa del plan de pruebas de continuidad de negocio.
- Coordinación de las actividades de auditora de continuidad de negocio.
- Coordinar los planes de mejora.