Política de Seguridad de la Información

ÍNDICE DE CONTENIDOS

1. APROBACIÓN Y ENTRADA EN VIGOR 3
2. INTRODUCCIÓN 3
3. LA AUTORIDAD PORTUARIA DE BALEARES 4
4. MARCO NORMATIVO 4
5. LA SEGURIDAD DE LA INFORMACIÓN 4
6. ALCANCE 6
7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 6
8. OBLIGACIONES DEL PERSONAL 6
9. TERCERAS PARTES 7
10. FORMACIÓN Y CONCIENCIACIÓN 7
11. GESTIÓN DE RIESGOS 8
12. DATOS DE CARÁCTER PERSONAL 8
13. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 8
14. ANEXO I. MARCO NORMATIVO 10
15. ANEXO II. ACRÓNIMOS 12

1. Aprobación y Entrada en Vigor

La Autoridad Portuaria de Baleares dispone de una Política de Seguridad de la Información aprobada por acuerdo en el Consejo de Administración de la Autoridad Portuaria de Baleares en sesión celebrada el 27 de Octubre de 2021.

La Política es de aplicación desde su fecha de aprobación hasta que sea reemplazada por una nueva.

El Comité de Seguridad de la Información revisará la Política de forma ordinaria con carácter anual y de forma extraordinaria cuando se produzcan cambios en la estructura de la Autoridad Portuaria de Baleares que así lo aconsejen.

La Autoridad Portuaria de Baleares pondrá a disposición los medios para dar a conocer y facilitar el cumplimiento de la Política y de las normativas que la desarrollan, así como para verificar su aplicación y efectividad.

2. Introducción

La "Política de Seguridad de la Información" aprobada por el Consejo de Administración de la Autoridad Portuaria de Baleares, en adelante APB, da cumplimiento al artículo 12 (Requisitos mínimos de Seguridad del Real Decreto 311/2022 de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica) y de la medida de seguridad org.1 contemplada en el Anexo II de dicho Real Decreto.

En este sentido, el mencionado artículo 12 establece que "*Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente.*"

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

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

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

Los sistemas de información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

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

ENS y LOPD-gdd), así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

3. La Autoridad Portuaria de Baleares

La Autoridad Portuaria de Baleares, organismo público con personalidad jurídica y patrimonio propio, que gestiona los cinco puertos de interés general de las Islas Baleares (Palma y Alcúdia en Mallorca, Maó en Menorca, Eivissa en la isla del mismo nombre y la Savina en Formentera) y que está adscrito al Ministerio de Transportes, Movilidad y Agenda Urbana a través del organismo público Puertos del Estado.

La Autoridad Portuaria de Baleares ejerce sobre sus puertos las competencias siguientes:

- Realización, autorización y control de las operaciones marítimas y terrestres relacionadas con el tránsito portuario y los servicios portuarios.
- Ordenación de la zona de servicio del puerto y de los usos portuarios.
- Planificación, proyecto, construcción, conservación y explotación de las obras de servicios del puerto y de las señales marítimas.
- Gestión del dominio portuario y de las señales marítimas.
- Fomento de las actividades industriales y comerciales relacionadas con el tránsito marítimo o portuario.
- Coordinación de las operaciones de las diferentes maneras de transporte en el espacio portuario.

Los órganos de gobierno de la Autoridad Portuaria de Baleares son:

- Consejo de Administración
- Presidencia
- Dirección

El detalle de cada uno de los anteriores órganos se describe en la Sede Electrónica de la Autoridad Portuaria de Baleares, concretamente *https://seu.portsdebalears.gob.es*

4. Marco Normativo

La normativa a la que se encuentra sometida la Autoridad Portuaria de Baleares, más relacionada con su actividad, se recoge en el Anexo I del presente documento.

5. La Seguridad de la Información

El objeto de la Política es establecer la postura de la APB respecto a la Seguridad que afecta a los procesos relacionados con el desempeño de sus funciones y, muy particularmente, con los relacionados con la administración electrónica, tanto desde el punto de vista de los usuarios de los servicios, como desde el punto de vista interno, para la gestión de la propia Entidad.

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

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

- el cumplimiento de los objetivos de su misión y de prestación de servicios
- el cumplimiento de la legislación y normativa aplicables

Para ello,

- se preverán y desplegarán medidas para evitar incidentes de seguridad que pudieran afectar al cumplimiento de objetivos o poner en riesgo las infraestructuras.
- se diseñarán medidas de respuesta ante incidentes de seguridad, físicos o lógicos, de forma que se minimice el impacto de los mismos, en caso de que ocurrieran.
- La protección de las infraestructuras frente ataques deliberados

Como norma general, se tendrá un enfoque de orientación al riesgo a la hora de diseñar las medidas de seguridad necesarias, poniendo más foco y esfuerzo en la mitigación de lo que suponga un mayor riesgo. No obstante, para la protección de las infraestructuras, también se tendrá en cuenta el impacto, desplegando medidas preventivas y de respuesta.

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

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

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

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

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

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

6. Alcance

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

7. Organización de la Seguridad de la Información

La seguridad en APB está soportada sobre una estructura de tres niveles:

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

La organización de la Seguridad de la Información, con la especificación de los roles y sus funciones, se especifica en el documento interno *APB STIC-POL-1 Política de Seguridad de la Información*.

8. Obligaciones del personal

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

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

9. Terceras Partes

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

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

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

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

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

10. Formación y Concienciación

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

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

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

El primer objetivo se asocia a formación y el segundo a concienciación.

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

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

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

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

11. Gestión de Riesgos

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

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

Todos los sistemas sujetos a la Política deberán ser objeto de un análisis de riesgos que evalúe las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá regularmente, al menos una vez al año, elevándose las conclusiones al Comité de Seguridad de la Información. Se realizará un análisis de riesgos de los sistemas de información en periodos inferiores a un año cuando:

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

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

12. Datos de carácter personal

La Autoridad Portuaria de Baleares solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la legislación vigente en materia de protección de datos personales.

13. Desarrollo de la Política de Seguridad de la Información

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

La aprobación y revisión de los documentos anteriormente reseñados se hará conforme a lo siguiente:

- Política de Seguridad de la Información: será aprobada por el Consejo de Administración, siendo responsabilidad del Comité de Seguridad de la Información su revisión para elevar, a través del Director, una propuesta de modificación cuando sea necesario.

- Normativa Interna de seguridad de la información: será revisada por el Comité de Seguridad de la Información, siendo el Responsable de Seguridad de la Información el responsable de su elaboración y actualización. La normativa interna de seguridad será aprobada por el Presidente, por delegación del Consejo de Administración, a propuesta del Comité de Seguridad de la Información.

- Procedimientos operativos de seguridad de la información: serán aprobados por el Director, previo informe favorable del Comité de Seguridad de la Información, a propuesta, de los responsables de los diferentes departamentos, divisiones, o del Responsable de Seguridad de la Información.

Toda la documentación generada por la Normativa Interna de seguridad de la información y Procedimientos operativos de seguridad de la información estará alineada con la Política del Sistema Integrado de Gestión (Calidad, Medio Ambiente y Documental).

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

14. Anexo I. Marco Normativo

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

- Real Decreto 371/1987, de 13 de marzo, por el que se aprueba el Reglamento para la ejecución del Real Decreto-ley 2/1986, de 23 de mayo, de estiba y desestiba.
- Ley 22/1988, de 28 de julio, de Costas
- Real Decreto 145/1989, de 20 de enero, por el que se aprueba el Reglamento Nacional de Admisión, Manipulación y Almacenamiento de Mercancías Peligrosas en los Puertos.
- Real Decreto 393/1996, de 1 de marzo, por el que se aprueba el Reglamento general de Practicaje, de conformidad con lo establecido en la Ley de Puertos del Estado y de la Marina Mercante.
- CÓDIGO INTERNACIONAL para la protección de los buques y de las instalaciones portuarias (Código PBIP), adoptadas el 12 de diciembre de 2002 mediante Resolución 2 de la Conferencia de Gobiernos contratantes del Convenio Internacional para la Seguridad de la Vida Humana en el Mar, 1974.
- Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.
- RESOLUCIÓN de 11 de octubre de 2006, de Puertos del Estado, por la que se dispone la publicación del acuerdo de su Consejo Rector, relativo a la aprobación del Pliego regulador del servicio portuario básico de amarre y desamarre de buques.
- Real Decreto 1617/2007, de 7 de diciembre, por el que se establecen medidas para la mejora de la protección de los puertos y del transporte marítimo.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- ORDEN FOM/938/2008, de 27 de marzo, que aprueba el pliego de condiciones generales para el otorgamiento de concesiones en el dominio público portuario estatal.
- Orden FOM/4003/2008, de 22 de julio, por la que se aprueban las normas y reglas generales de los procedimientos de contratación de Puertos del Estado y Autoridades Portuarias.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Real Decreto 4/2010, de 3 de mayo, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto Legislativo 2/2011, de 5 de septiembre, por el que se aprueba el Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante.
- Orden FOM/1698/2013, de 31 de julio, por la que ese modifica la Orden FOM/4003/2008, de 22 de julio, por la que se aprueban las normas y reglas generales de los procedimientos de contratación de Puertos del Estado y Autoridades Portuarias.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Orden HAP/2425/2013, de 23 de diciembre, por la que se publican los límites de los distintos tipos de contratos a efectos de la contratación del sector público a partir del 1 de enero de 2014.

- Real Decreto-ley 8/2014, de 4 de julio, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
- Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia.
- Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos
- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre de Régimen Jurídico del Sector Público.
- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- Real Decreto 130/2017, de 24 de febrero, por el que se aprueba el Reglamento de Explosivos.
- Orden HFP/1298/2017, de 26 de diciembre, por la que se publican los límites de los distintos tipos de contratos a efectos de la contratación del sector público a partir del 1 de enero de 2018
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley 6/2020, DE 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- 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.

Así como la Legislación que sustituya o complete las disposiciones citadas y la nueva legislación aplicable que se promulgue.

15. Anexo II. Acrónimos

APB	Autoridad Portuaria de Baleares
ENS	Esquema Nacional de Seguridad
CCN	Centro Criptológico Nacional
CNPIC	Centro Nacional de Protección de Infraestructuras Críticas
LOPD-gdd	Ley Orgánica de Protección de Datos y garantía de derechos digitales
PSO	Plan de Seguridad del Operador
TIC	Tecnologías de la Información y las Comunicaciones
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones

En base al RD 3/2010 de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, se describe como:

Normativa de Seguridad (org.2)

Una serie de documentos que describen:

- El uso correcto de equipos, servicios e instalaciones.
- Lo que se considerará uso indebido.
- La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Procedimiento de Seguridad (org.3)

Una serie de documentos que detallan de forma clara y precisa:

- Cómo llevar a cabo las tareas habituales.
- Quién debe hacer cada tarea.
- Cómo identificar y reportar comportamientos anómalos.