MINISTERIO
DE TRANSPORTES
Y MOVILIDAD SOSTENIBLE

ALICANTE PORT
Autoridad Portuaria de Alicante

Patricia Fernández Porto (1 de 2)
Responsable de Sistemas de Información y Comunicaciones
Fecha Firma: 03/08/2026
HASH: e70200f082bc548607ae52c3abb8e3720

SERGIO SANCHEZ JURADO (2 de 2)
Jefe de Departamento para la Transformación Digital
Fecha Firma: 04/08/2026
HASH: be13e7ffc9d3c65442604b55a31a570f

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
Autoridad Portuaria de Alicante

Código:	POL-ENS-01
Fecha:	24/07/2026
Versión:	2.0
Clasificación:	USO PÚBLICO

Cód. Validación: 9QHKZRSCDQMPH4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 1 de 16

HOJA DE ESTADO DEL DOCUMENTO

Versión	Fecha	Págs.	Preparado	Cambios
1.0	16/03/2026	17	OFICINA TÉCNICA S.I.- GMV	Primera versión de la PSI
2.0	24/07/2026	17	OFICINA TÉCNICA S.I.- GMV	ANEXO I: Identificación, seguimiento y actualización de la normativa aplicable a través de un “Registro”, REG-ENS-00-04_Registro_Normativa_v1”

CONTROL DE APROBACIÓN DEL DOCUMENTO

Revisado por:	Revisado por:	Aprobado por:
Responsable de Seguridad de la Información	Comité de Seguridad de la Información	Consejo de Administración
Fecha: 03/08/2026	Fecha: 03/08/2026	Fecha: 23/03/2026

Cód. Validación: 9QHKZRSCDQMPH4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 2 de 16

ÍNDICE

Cód. Validación: 9QHKZRSCDQMPH4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 3 de 16

1. INTRODUCCIÓN

La Autoridad Portuaria de Alicante depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) 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 Autoridad Portuaria de Alicante 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 el organismo 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 en todos los ámbitos en que se organiza la Autoridad Portuaria de Alicante se apliquen las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, 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.

Toda la estructura de la Autoridad Portuaria de Alicante debe 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.

Los objetivos establecidos por la Autoridad Portuaria de Alicante son los siguientes:

- Realización, autorización y control de las operaciones marítimas y terrestres relacionadas con el tráfico 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 y servicios del puerto y de las señales marítimas.
- Gestión del dominio público portuario y de las señales marítimas.
- Optimización de la gestión económica y rentabilización del patrimonio y recursos del puerto.
- Fomento de actividades industriales y comerciales relacionadas con el tráfico marítimo o portuario.
- Coordinación de las operaciones de las distintas modalidades de transporte en el espacio portuario.

La seguridad de la información garantiza que la Autoridad Portuaria de Alicante pueda cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, se elabora la presente Política, sobre la base de los siguientes principios básicos:

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, conforme a la normativa que regula al organismo público.

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.

Cód. Validación: 9QHKZRSCDQMPT4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 4 de 16

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. En todo caso, la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

Cód. Validación: 9QHKZRSCDQMPH4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 5 de 16

2. ALCANCE

Esta política se aplica a todos los sistemas TIC de la Autoridad Portuaria de Alicante y a todos los miembros de la organización. Específicamente, se aplica a los sistemas TIC que dan soporte a los servicios/información prestados por el organismo público, al ejercicio de derechos y cumplimiento de deberes por medios electrónicos, y a la interacción por medios electrónicos con los ciudadanos y la Comunidad Portuaria. Asimismo, respetando el marco normativo aplicable del organismo, se aplica a la interacción por medios electrónicos con el resto del sector público.

La misma será de obligado cumplimiento para todo el personal que tenga acceso a dichos sistemas, ya sean empleados del sector público o no. Siendo imperativo que cada usuario conozca y siga las disposiciones establecidas en este documento y las normativas de seguridad vigentes.

La Autoridad Portuaria de Alicante, a propuesta del Comité de Seguridad de la Información, 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 Esquema Nacional de Seguridad.

3. MISIÓN DE LA ORGANIZACIÓN

La Misión de la Autoridad Portuaria de Alicante será contribuir al desarrollo económico y social del área de influencia del puerto, mediante la prestación de servicios eficientes y sostenibles que ayuden a mejorar la competitividad de sus clientes y que generen valor añadido que pueda ser compartido con la sociedad.

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, publicado en el BOE núm. 253, de 20 de octubre de 2011, siendo estas las siguientes:

a) 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.
b) 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.
c) 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.
d) La gestión del dominio público portuario y de señales marítimas que les sea adscrito.
e) La optimización de la gestión económica y la rentabilización del patrimonio y de los recursos que tengan asignados.
f) El fomento de las actividades industriales y comerciales relacionadas con el tráfico marítimo o portuario.
g) La coordinación de las operaciones de los distintos modos de transporte en el espacio portuario.
h) La ordenación y coordinación del tráfico portuario, tanto marítimo como terrestre.

4. MARCO LEGAL Y REGULATORIO

El presente apartado define las responsabilidades legales y regulatorias de la Autoridad Portuaria de Alicante 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 la actividad prestada por la Autoridad Portuaria de Alicante.
- **Obligaciones Contractuales con Terceros**: En el ámbito de la normativa de contratación aplicable al organismo público, reconocerá y cumplirá con las disposiciones establecidas en los acuerdos con organismos y entidades de todo tipo, proveedores 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

Cód. Validación: 9QHKZRSCTQMPHENS2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 6 de 16

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 Autoridad Portuaria de Alicante estén alineadas con estos requisitos legales y regulatorios.

El presente epígrafe busca garantizar que todas las actividades relacionadas con la información dentro de la Autoridad Portuaria de Alicante 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 Autoridad Portuaria de Alicante en materia de seguridad de la información viene recogido en el “ANEXO I: MARCO NORMATIVO”.

5. ORGANIZACIÓN DE LA SEGURIDAD

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

Para garantizar el cumplimiento del ENS, la Autoridad Portuaria de Alicante 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.

5.1. ROLES: FUNCIONES Y RESPONSABILIDADES

La Autoridad Portuaria de Alicante ha designado 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
- Responsable del Sistema
- Coordinador de Continuidad y Gestión de Crisis

Adicionalmente, la APA ha constituido el Comité de la Seguridad de la Información. Los roles, funciones y responsabilidades se detallan en la presente política en el ANEXO II: ROLES: FUNCIONES Y RESPONSABILIDADES.

En caso de existir conflictos relacionados con sus competencias en el ámbito de la seguridad de la información entre los distintos responsables designados, estos conflictos serán comunicados al Comité de Seguridad de la información desde el cual se evaluarán y se propondrán soluciones a los mismos. En caso de no ser aceptadas dichas soluciones por las partes implicadas se escalará la decisión final a la Presidencia de la Autoridad Portuaria.

5.2. COMITÉ: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad de la Información (en adelante CSI) es el órgano que dentro de la Autoridad Portuaria de Alicante coordina al más alto nivel la Seguridad de la Información.

El CSI estará constituido por los siguientes miembros:

- **Presidencia del CSI:** Presidente de la Entidad
- **Vicepresidencia del CSI**: Director de la Entidad
- **Secretaría:** Secretario General de la Autoridad Portuaria
- **Vocales:**
  - Responsables de los Servicios y de la Información
  - Responsable del Sistema
  - Responsable de Seguridad de la Información
  - Coordinador de Continuidad y Gestión de Crisis
  - Delegado de Protección de Datos
- **Terceros invitados** (con voz, pero sin voto): Personal interno o externo en función de la orden del día.

Cód. Validación: 9QHKZRSCDQMPH4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 7 de 16

Podrán ser invitados al CSI, con voz, pero sin voto, y en función de las circunstancias, cualquier persona de la Autoridad Portuaria de Alicante implicado en alguno de los aspectos relativos a la Seguridad de la Información, y siempre y cuando el Presidente del Comité lo considere adecuado.

El Vicepresidente del Comité asumirá las responsabilidades del Presidente en caso de ausencia.

Los Responsables de los Servicios y de la Información serán convocados en función de los asuntos a tratar, pudiendo el CSI recoger las funciones y obligaciones de los Responsables de los Servicios y de la Información, en aquellas acciones transversales en las que le sea solicitado y/o se considere necesario.

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

El CSI reportará regularmente del estado de la seguridad de la información a la Presidencia.

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

5.3. PROCEDIMIENTO DE DESIGNACIÓN

La Autoridad Portuaria de Alicante designará formalmente mediante resolución del Presidente, a los siguientes miembros del CSI: Responsable de Seguridad de la Información, Responsables de los Servicios y de la Información, Coordinador de Continuidad y Gestión de Crisis y Responsable del Sistema.

El CSI quedará formalmente constituido mediante la aprobación del documento “Designación de Roles y Constitución del Comité de Seguridad”.

Todos estos nombramientos serán puestos en conocimiento de los responsables mediante el correspondiente documento “Notificación de nombramiento de roles y funciones”, donde las personas designadas serán notificadas e informadas de las responsabilidades que acompañan al rol a ejercer.

6. DATOS DE CARÁCTER PERSONAL

En el desarrollo de sus funciones, la Autoridad Portuaria de Alicante maneja datos personales por lo que, en cumplimiento de la normativa vigente, aplicará las medidas técnicas y organizativas apropiadas que garanticen un tratamiento conforme a la normativa aplicable.

Así mismo, todos los sistemas de información de la Autoridad Portuaria de Alicante cumplirán con los niveles de seguridad establecidos por el Esquema Nacional de Seguridad de 2022, el Reglamento General de Protección de Datos (RGPD) y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, asegurando así la protección de los datos personales desde el diseño y por defecto.

Consecuencia de lo anterior, el Delegado de Protección de Datos es miembro nato del CSI.

7. GESTIÓN DE RIESGOS

En relación con todos los sistemas de información incluidos en el alcance de esta Política, se debe realizar un análisis de riesgos que evalúe las amenazas y riesgos a los que están expuestos, incluyendo aquellos exigidos por la normativa de 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 Esquema Nacional de Seguridad y 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 de seguridad de alto impacto para la organización.
- Cuando se reporten vulnerabilidades críticas.

Para la armonización de los análisis de riesgos, el CSI establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

8. AUDITORÍA

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

Cód. Validación: 9QHKZRSCDQMPH4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 8 de 16

- Ordinaria: Periodo bienal.
- Extraordinaria: Siempre que se produzcan modificaciones sustanciales, entendidas como aquellos cambios que puedan alterar de forma significativa su arquitectura, funcionalidad o nivel de exposición, y que puedan tener impacto en la eficacia o adecuación de las medidas de seguridad establecidas conforme al Esquema Nacional de Seguridad. 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.

9. OBLIGACIONES DEL PERSONAL

Todo el personal de la Autoridad Portuaria de Alicante está obligado a conocer y cumplir con esta Política y la Normativa de Seguridad, siendo responsabilidad del CSI proponer las medidas adecuadas para que esta información llegue a todos los empleados afectados.

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 Autoridad Portuaria de Alicante, 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 Política y de la 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.

10. TERCERAS PARTES

Cumpliendo el marco normativo que regula el sector público, en las ocasiones en que la Autoridad Portuaria de Alicante preste servicios o maneje información de otros entes u organismos públicos, se les informará sobre esta Política. Además, se crearán canales de reporte y coordinación entre los miembros de los respectivos Comité de Seguridad de la Información de cada ente, y se establecerán procedimientos conjuntos para la respuesta ante incidentes de seguridad.

Cuando la Autoridad Portuaria de Alicante reciba servicios de terceros o comparta información con terceros, se les informará de esta Política, de la 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. Los terceros deberán garantizar que su personal esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política 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 los Servicios y de la Información afectados antes de seguir adelante.

11. ESTRUCTURA DE LA DOCUMENTACIÓN

La documentación relativa a la gestión de la Seguridad de la Información, que recoge las directrices, normas, procedimientos y registros necesarios para garantizar el cumplimiento del Esquema Nacional de Seguridad (ENS), se clasificará en cuatro niveles jerárquicos, organizados de forma estructurada para facilitar su implantación, revisión y control:

- **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.

Cód. Validación: 9QHKZRSCDQMPH4EN6S2FSEXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 9 de 16

11.1. 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 la Presidencia del 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.

11.2. 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 aprobación de la documentación redactada en este nivel corresponde al CSI, a propuesta del Responsable de Seguridad. Se garantiza así la correcta alineación con la Política de Seguridad de la Información y los requisitos legales y técnicos pertinentes.

11.3. 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 al Responsable del Sistema, en coordinación con el Responsable de Seguridad.

11.4. 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 generación y mantenimiento de esos documentos los coordinará el Responsable del Sistema.

11.5. 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.

12. VALIDEZ DEL DOCUMENTO

Este documento constituye la versión actualizada de la Política de Seguridad de la Información de la Autoridad Portuaria de Alicante. La validez de esta política se extiende desde la firma de esta, hasta la próxima revisión que realice el CSI 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 el Presidente de la Autoridad Portuaria de Alicante, dando cuenta de este al Consejo de Administración.
- Estará sujeta a una revisión anual regular.
- Deberá revisarse cuando se detecten cambios significativos en la Autoridad Portuaria de Alicante.

La revisión anual de la presente Política corresponde al Comité de Seguridad de la Información proponiendo en caso de que sea necesario mejoras de esta.

La efectiva gestión y cumplimiento de esta política 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.

Cód. Validación: 9QHKZRSCDQMPH4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 10 de 16

13. ANEXO I: IDENTIFICACIÓN, SEGUIMIENTO Y ACTUALIZACIÓN DE LA NORMATIVA APLICABLE

La presente sección establece el procedimiento de identificación de la legislación aplicable y de actualización permanente de un registro donde se conservan referencias a dichas normas actualizadas, así como las actividades necesarias para la identificación, seguimiento, evaluación y actualización de la normativa legal y regulatoria aplicable a la seguridad de la información en la Autoridad Portuaria de Alicante, con el fin de mantener actualizado el registro de normativa aplicable y garantizar el cumplimiento del Esquema Nacional de Seguridad.

La responsabilidad de la identificación, seguimiento y actualización de la normativa aplicable recae en el Responsable de la Seguridad de la Información, quien velará por la adecuada vigilancia normativa y por la actualización de los registros asociados, de acuerdo con lo establecido en este procedimiento.

La identificación de cambios normativos se realiza mediante el seguimiento periódico de fuentes oficiales y de referencia, relacionadas con el Esquema Nacional de Seguridad, la seguridad de la información, la protección de datos y la ciberseguridad, incluyendo, al menos, las siguientes:

- Boletín Oficial del Estado (BOE) y, en su caso, boletines oficiales autonómicos.
- Diario Oficial de la Unión Europea (DOUE).
- Publicaciones, guías y comunicaciones del Centro Criptológico Nacional (CCN), incluyendo:
    - Guías y documentos de la serie CCN-STIC.
    - Comunicados, alertas y avisos de seguridad del CCN-CERT.
- Información publicada por el Instituto Nacional de Ciberseguridad (INCIBE).
- Comunicaciones y resoluciones de autoridades competentes en materia de seguridad de la información y protección de datos.
- Otras fuentes oficiales que puedan resultar aplicables al contexto de actividad de la Autoridad Portuaria de Alicante.

Los cambios normativos detectados son analizados por el Responsable de la Seguridad de la Información para determinar su aplicabilidad al ámbito de actividad de la Autoridad Portuaria de Alicante y su impacto sobre la Política de Seguridad de la Información, la normativa interna, los procesos y las medidas de seguridad implantadas. Como resultado de dicho análisis, se definirán, cuando proceda, las acciones necesarias para asegurar la adecuación al marco normativo vigente.

La Autoridad Portuaria de Alicante mantiene un registro de normativa aplicable en el que se documenta, al menos, la identificación de la norma, su estado de vigencia y el resultado del análisis de aplicabilidad e impacto. Dicho registro constituye la referencia para el seguimiento normativo y se mantiene actualizado conforme a este procedimiento.

Asimismo, la Autoridad Portuaria de Alicante dispone de un registro específico de bases legales aplicables, identificado como REG-ENS-00-04, gestionado por el Responsable de la Seguridad de la Información a través del gestor documental corporativo. Este registro garantiza la trazabilidad, el control de versiones, la integridad y la disponibilidad de la documentación normativa relacionada con el Esquema Nacional de Seguridad y la seguridad de la información.

El procedimiento y el registro asociado serán revisados de forma periódica y de manera extraordinaria cuando se produzcan cambios normativos relevantes, modificaciones significativas en el contexto organizativo o como resultado de auditorías o revisiones del sistema de seguridad.

La Autoridad Portuaria de Alicante mantiene, asimismo, un registro específico de bases legales aplicables, gestionado a través de su gestor documental corporativo, que garantiza la trazabilidad, control de versiones y disponibilidad de la documentación normativa. La gestión, actualización y conservación de dicho registro y de la documentación asociada se realizará conforme a la presente sección y al procedimiento PRO-ENS-21 Procedimiento de Gestión Documental.

14. ANEXO II: ROLES: FUNCIONES Y RESPONSABILIDADES.

14.1. FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Son funciones típicas del Comité de Seguridad de la Información (CSI):

Cód. Validación: 9QHKZRSCDQMPH4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 11 de 16

- Atender las inquietudes de los órganos rectores de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a los órganos rectores.
- 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 los diferentes ámbitos 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 para su aprobación por los órganos rectores.
- Aprobar la Normativa y Procedimientos 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.
- 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.
- Coordinación y supervisión al más alto nivel del cumplimiento de la normativa 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).

14.2. 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.

14.2.1. MÁXIMA AUTORIDAD DEL ORGANISMO PÚBLICO

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, 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 y en resto del ordenamiento jurídico aplicable.

El Titular de Autoridad Portuaria de Alicante, apoyado por los Responsables de los 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 Política de Seguridad de la Información 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.

Cód. Validación: 9QHKZRSCDQMPH4EN8S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 12 de 16

14.2.2. RESPONSABLE DE LA INFORMACIÓN

El Responsable de la Información será designado por el Presidente del organismo público. Sus funciones serán las siguientes:

- 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.
- Proponer al CSI el establecimiento de 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.

14.2.3. RESPONSABLE DEL SERVICIO

El Responsable del Servicio será designado por el Presidente del organismo público. Sus funciones serán las siguientes:

- El Responsable del Servicio es el responsable último de cualquier error o negligencia que lleve a un incidente de disponibilidad de los servicios.
- Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
- 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.
- Proponer al CSI el establecimiento de 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.

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 la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

14.2.4. 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 Política de Seguridad de la Información de la organización.
- 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 su 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.

Cód. Validación: 9QHKZRSCDQMPH4ENBS2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 13 de 16

- 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.
- Propondrá a la Presidencia del CSI, la convocatoria del Comité de Seguridad de la Información (CSI), 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 Política de Seguridad de la Organización.
- 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 del 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 responsables 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, de las Normativas de Seguridad de la Información.
- Participará en la elaboración y aprobación, en el marco del CSI, de los Procedimientos Operativos de Seguridad de la Información.
- Facilitará periódicamente al CSI 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.
- Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el CSI.
- Validará los Planes de Continuidad de Sistemas que elabore el responsable de Sistemas, que deberán ser aprobados por el CSI y probados periódicamente por el responsable del Sistema.
- 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.

14.2.5. RESPONSABLE DEL SISTEMA

El Responsable del Sistema se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el responsable de Seguridad de la Información.
Las funciones del Responsable del Sistema 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.
- Elaborar y aprobar los procedimientos técnicos de seguridad.
- 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:

Cód. Validación: 9QHKZRSCDQMPH4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 14 de 16

- 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.

14.2.6. 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.

Las funciones del Delegado de Protección de Datos son las generales establecidas en la normativa sectorial, destacando específicamente en cuanto a la Política de Seguridad de la Información 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.

Cód. Validación: 9QHKZRSCDQMPH4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 15 de 16

- 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, en su caso, 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.

14.2.7. COORDINADOR DE CONTINUIDAD Y GESTIÓN DE CRISIS

En la Autoridad Portuaria de Alicante se designará formalmente un Coordinador de Continuidad y Gestión de Crisis, quien será el encargado de coordinar la respuesta institucional ante situaciones de alto impacto para asegurar la continuidad del negocio. 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. Sus funciones principales son las siguientes:

- Activación del Plan de Continuidad y Gestión de Crisis.
- Bajo el criterio del Coordinador de Continuidad y Gestión de Crisis, podrá solicitar a diferentes perfiles según la naturaleza y nivel de la 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, esta actividad podrá delegarse en otros miembros operativos.
- Elaboración del informe final de crisis en colaboración con el resto de integrantes del CSI y equipo participante.
- Cierre de la crisis.
- Coordinación del programa del plan de pruebas de continuidad de negocio.
- Coordinación de las actividades de auditoría de continuidad de negocio.
- Coordinar los Planes de mejora.

Cód. Validación: 9QHKZRSCDQMPH4EN6S2F3EXGG
Verificación: https://sede.puertoalicante.gob.es/
Documento firmado electrónicamente desde la plataforma esPublico Gestiona | Página 16 de 16