Port Tarragona

Referència: SECRETARIA/YVC/nrp
6.1 20.12.23

Sr. Director general
Autoritat Portuària

Aprovació de la Política de Seguretat de la Informació de l'Autoritat Portuària de Tarragona.

El Consell d'Administració d'aquesta Autoritat Portuària, en la sessió de 20 de desembre de 2023 va adoptar el següent acord:

"Vist que l'article 12 "Política de Seguridad y requisitos mínimos de Seguridad", del Reial Decret 311/2022, de 3 de maig, pel qual es regula l' Esquema Nacional de Seguretat, estableix que la política de seguretat serà aprovada per l'òrgan competent que correspongui.

Vista la proposta del director general de l'Autoritat Portuària de data 14 de desembre de 2023 al respecte.

Atès el que disposa l'article 30.5 del text refós de la Llei de ports de l'Estat i de la marina mercant (RDL 2/2011, de 5 de setembre) s'acorda:

Primer.- Aprovar la Política de Seguretat de la Informació de l'Autoritat Portuària de Tarragona i que s'adjunta al present acord.

Segon.- Facultar al director general de tal de poder subscriure els nomenaments i l'aprovació d'aquells temes i documents relacionats."

D'acord amb el que preveu l'art. 19.5 de la Llei 40/2015, d'1 d'octubre, de Règim Jurídic del Sector Públic, es fa constar que el present acord ha estat emès amb anterioritat a l'aprovació de l'Acta de la sessió en la qual es va adoptar.

El present document ha estat signat electrònicament per Saül Garreta Puig i per Yolanda Vizcarro Caparrós en la seva condició de president i secretària, respectivament, del Consell d'Administració de l'Autoritat Portuària de Tarragona, en la data que consta en la validació del mateix, validació que pot ser verificada mitjançant el Codi Segur de Verificació (CSV) que també inclou.

1. INTRODUCCIÓN

La Autoridad Portuaria de Tarragona, (en adelante APT), depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos institucionales. 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, confidencialidad, autenticidad y trazabilidad de la información tratada o los servicios prestados.

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 ante cualquier incidente.

Los sistemas TIC 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 la APT y su personal debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, (en adelante ENS) y la norma internacional ISO/IEC 27001:2022, 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 APT 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 las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

La APT debe estar preparada para prevenir, detectar, dar respuesta y conservar la información necesaria con el fin de minimizar las vulnerabilidades y eliminar o reducir las amenazas antes de que se materialicen, de acuerdo al Artículo 8 del ENS.

En virtud de lo expuesto, la Política de Seguridad de la Información para la APT se regirá por los siguientes puntos.

2. OBJETIVOS

El objetivo de este documento es constituir la Política de Seguridad de la Información para la APT, entendiéndose en todos los casos la seguridad como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información de tramitación electrónica.

Dar a conocer a todo el personal de la APT la presente política y la certificación de la organización en relación con el ENS y la norma ISO/IEC 27001.

La política debe de ser conocida y cumplida por todo el personal de la APT, independientemente del puesto, cargo y responsabilidad dentro de la misma.

3. PREVENCIÓN

La APT debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello la APT debe implementar las medidas mínimas de seguridad determinadas por el ENS y la norma ISO/IEC 27001, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, la APT debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

4. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continuada para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los

responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

5. RESPUESTA

La APT debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos de la APT.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

6. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, la APT debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

7. ALCANCE

Esta política se aplica a todos los sistemas TIC que están bajo la prestación de los servicios de la administración electrónica, en especial a la sede electrónica de la APT, y a todos los miembros de la organización, sin excepciones, que estén bajo este alcance. Es de cumplimiento por todo el personal de la APT.

De forma concreta, la presente Política de Seguridad es aplicable sobre las TIC y **los sistemas de información relacionados con los servicios de detección y respuesta de ataques, protección de sitios web, detección de amenazas, supervisión y administración de la seguridad a través del SOC y análisis de vulnerabilidades, con el fin de dar soporte a los procesos de: gestión de la atención al cliente/usuario, gestión de proyectos, gestión operativa y diseño y planificación, de acuerdo con la declaración de aplicabilidad vigente.**

La organización desestima la aplicación de la presente Política de Seguridad de la Información sobre aquellos sistemas de información no reflejados en este apartado.

8. MISIÓN

Corresponden a la APT las competencias y funciones establecidas en los artículos 25 y 26 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 la Marina Mercante.

De igual modo la APT tiene como principal misión respetar y cumplir los principios de seguridad en materia del ENS y la norma ISO/IEC 27001:

- La seguridad como un proceso integral.
- Gestionar de la seguridad basada en los riesgos.
- Prevención, reacción y recuperación de la seguridad física y lógica.
- Establecer líneas de defensa respecto a la seguridad de la información para ofrecer uno servicios seguros.
- Reevaluación periódica del cumplimiento legal.
- La seguridad como función diferenciada.
- Velar por el cumplimiento legal.
- Proporcionar un marco de referencia para el establecimiento de los objetivos de seguridad de la información.
- Velar por la mejora continua del sistema de gestión de seguridad de la información.

9. MARCO NORMATIVO

Son de aplicación las leyes y normativas españolas en relación con protección de datos personales, propiedad intelectual y uso de herramientas telemáticas. Por todo ello, la APT podrá ser requerida por los órganos administrativos pertinentes a proporcionar los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

La principal normativa que es de aplicación se especifica a continuación:

- 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.

- 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, por el que se regula el Esquema Nacional de Seguridad.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la Información y Comercio Electrónico (LSSI).
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- REGLAMENTO (UE) Nº 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014.
- 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.
- ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad.

10. ORGANIZACIÓN DE LA SEGURIDAD

La responsabilidad esencial recae sobre la Dirección General de la organización, ya que esta es responsable de organizar las funciones y responsabilidades y de facilitar los recursos adecuados para conseguir los objetivos del sistema de seguridad de la información. Los directivos son también responsables de dar buen ejemplo siguiendo las normas de seguridad establecidas.

Perfil	Cargo	Sustituto
Responsable de la Información	Jefe de Departamento de Servicios Jurídicos	Responsable de Secretaria General
Responsable del Sistema	Director de Sistemas de Información	Jefe de División de Sistemas de Información
Responsable de Seguridad	Jefe de División de Sistemas de Información	Director de Sistemas de Información
Responsable del Servicio	Responsable de Sistemas de Información	Responsable de Sistemas de Información-2

Dentro de la APT se cuentan con los siguientes roles y funciones:

Responsable de Seguridad

a) Establecer los requisitos de la información y de los servicios en materia de seguridad y gestionar la misma en función de lo establecido en las políticas y normativas aplicables al sistema de gestión de seguridad de la información.

b) Fomentar y participar en el desarrollo e implantación de la política del Sistema de la Información y su normativa, procedimiento o documentación derivada.

c) Coordinación de personal de seguridad dentro de la organización.

d) Aprobación final de las decisiones y comités de seguridad para su elevación a la Dirección General.

e) Trasladar a la Dirección General las decisiones en materia de seguridad de la información, así como los posibles incidentes detectados.

f) Mantener contacto con grupos de interés y autoridades en materia de seguridad informática para mantener actualizados los conocimientos de la compañía en esta materia y promover posibles iniciativas.

g) Velar por la efectividad de los controles implantados en la infraestructura tecnológica.

h) Asegurar los recursos y necesidades para asegurar la continuidad de los servicios y trasladar las necesidades a la Dirección General.

Responsable de la Información y del Servicio

a) Aprobación de manera formal de los niveles de la información y los servicios.

b) Proponer el diseño de acciones de concienciación y sensibilización relativas a la seguridad y dirigidas a todo el personal.

c) Mantener contacto con grupos de interés y autoridades en materia de seguridad de la información para mantener actualizados los conocimientos de la compañía en esta materia y promover posibles iniciativas.

d) Revisar los controles implantados en la infraestructura tecnológica.

e) Coordinar las pruebas oportunas para que la infraestructura funcione correctamente.

f) Liderar las posibles pruebas que se puedan realizar o auditorías técnicas u organizativas para evaluar el estado de los sistemas

Responsable del Sistema

a) Colaborar en la designación de los niveles de la información y los servicios.

b) Asegurar y velar por el funcionamiento de las plataformas informáticas y de seguridad e infraestructura tecnológica.

c) Colaborar en la dignación de medidas técnicas y organizativas en el ámbito de adecuación del sistema.

d) Gestionar la implementación de controles técnicos junto con el Responsable de la Información y del Servicio.

e) Escalar los posibles incidentes de seguridad de la información que afecten a los sistemas de seguridad de la información o que puedan afectar de forma indirecta.

f) Colaborar en la realización de auditorías técnicas u organizativas para evaluar el estado de los sistemas.

10.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

El Comité de Seguridad de la Información es el órgano decisorio en materia de seguridad de la información. Será el órgano responsable de proporcionar las directrices de gestión de la seguridad de la información en los servicios de la administración electrónica, y en especial en la sede electrónica de la APT.

Estará formado por el Responsable de Seguridad, el Responsable de la Información, el Responsable del Servicio y el Responsable del Sistema. El Comité tendrá las siguientes funciones:

a) Definir los objetivos y metas de la organización en materia de seguridad de la información y asegurar que los mismos están en conexión con los requisitos de negocio, procesos más relevantes, así como las normativas de calidad implantadas en la organización.

b) Formular, revisar y promulgar la política de seguridad de la información en la organización supervisando su efectiva implantación.

c) Establecer las directrices y apoyo de la organización a las iniciativas en materia de seguridad de la información.

d) Proveer a la organización de los recursos necesarios para acometer las actividades e implantar los controles necesarios relativos a la seguridad de la información.

e) Aprobar las obligaciones y funciones que se establezcan dentro de la organización en materia de seguridad de la información.

f) Promocionar la elaboración de planes y programas de formación en materia de seguridad de la información para su conocimiento por parte del personal de la organización.

g) Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.

h) 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 incidentes de seguridad de la información.

i) Asegurarse que la implementación de los controles y salvaguardas está coordinada y es extensiva a toda la organización.

j) Supervisar los cambios significativos y la exposición de los activos informáticos a amenazas significativas mediante la gestión del riesgo efectivo de la organización.

k) Revisar los incidentes de seguridad de la información relevantes.

l) Cumplir con las funciones y obligaciones que en materia de protección de datos de carácter personal en función de la legislación vigente.

m) Cumplir con las funciones y obligaciones que en materia de recuperación de desastres y continuidad del negocio han sido asignadas dentro del Plan de Contingencias al Comité de Crisis.

n) Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

o) Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.

p) Informar regularmente del estado de la seguridad de la información a la Alta Dirección.

q) Promover la mejora continua del sistema de gestión de la seguridad de la información.

El Comité de Seguridad de la Información reportará directamente a la Dirección General.

10.2. PROCEDIMIENTOS DE DESIGNACIÓN

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

En caso de conflicto entre los diferentes responsables, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Responsable de Seguridad.

Por la presente, la Dirección de APT asume la responsabilidad final y última del cumplimiento de la política.

11. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad de la Información la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Consejo de Administración de la APT y difundida para que la conozcan todas las partes afectadas.

12. DATOS DE CARÁCTER PERSONAL

La APT trata los datos de carácter personal conforme a la legislación vigente en materia de protección de datos.

La APT establece e implementa las medidas necesarias para dar al cumplimiento del reglamento como:

- Registro de actividades de tratamiento como responsable y encargado.
- Información disponible para los interesados y posibilidad de ejercer sus derechos y deberes.
- Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- La seudoanimización y el cifrado de datos personales, siempre que sea posible.

- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
- El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas asegurar el tratamiento.
- Procedimiento de quiebras de seguridad.

13. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se revisa regularmente:

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

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

14. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de la APT en diferentes materias:

- Organización e implantación del proceso de seguridad.
- Análisis y gestión de los riesgos.
- Gestión de personal o RRHH.
- Autorización y control de los accesos.
- Protección de las instalaciones.
- Gestión operativa.

- Protección y gestión de la infraestructura lógica.
- Protección de la información almacenada y en tránsito.
- Prevención ante otros sistemas de información interconectados.
- Registro de actividades.
- Incidentes de seguridad.
- Continuidad del sistema.
- Mejora continua.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. La normativa de seguridad estará disponible en la intranet.

14.1. OBLIGACIONES DEL PERSONAL

Todo el personal de la APT tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todo el personal de la APT deberá tener 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 todo el personal de la APT, 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.

15. TERCERAS PARTES

Cuando la APT preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la APT utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad de la Información que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de

incidencias. Se garantizará que el personal de terceros está 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 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 y los servicios afectados antes de seguir adelante.

16. CONTROL DE CAMBIOS

Descripción:	Autor:	Fecha:	Aprobado:	Fecha:	Versión
Adaptación a plantilla	R. Seguridad	03/01/2019			1
Revisión	R. Seguridad	03/05/2019			2
Revisión	R. Seguridad	15/03/2021			2
Integración ISO 27001 y ENS. Actualización nuevas versiones 2022	R. Seguridad	05/12/2023			3