POLITICA DE SEGURIDAD AUTORIDAD PORTUARIA DE MELILLA

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 16 de julio de 2015 por el consejo de Administración de la Autoridad Portuaria de Melilla.

Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN

La Autoridad Portuaria de Melilla depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. 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.

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 TIC 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 una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar 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.

Los diferentes departamentos 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.

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS. En virtud de lo expuesto, la Política de Seguridad de la Información de la Autoridad Portuaria de Melilla se regirá por las siguientes normas:

3. ALCANCE Y OBLIGACIONES DEL PERSONAL

El objeto de este documento es la aprobación de la Política de Seguridad de la Información, en adelante Política de Seguridad, del Organismo público Autoridad Portuaria de Melilla, y el establecimiento de un marco organizativo y tecnológico de la misma.

Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos y materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

Esta política se aplica a todos los sistemas TIC de la Autoridad Portuaria de Melilla y a todos los miembros de la organización, sin excepciones, debiendo ser conocida y cumplida por todo el personal de la Autoridad Portuaria de Melilla, independientemente del puesto, cargo y responsabilidad dentro del mismo.

4. MISIÓN

Corresponden a la Autoridad Portuaria de Melilla 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.

5. MARCO NORMATIVO

– Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

– Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

– Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

– Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

– Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

– 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.

– Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común.

– Ley 59/2003, de 19 de diciembre, de firma electrónica.

– Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. Comité de Seguridad

Para la gestión de la Seguridad de la Información, se crea el Comité de Gestión de la Seguridad de la Información, en adelante el Comité de Seguridad, dentro del ámbito de la presente Política de Seguridad que coordinará las actividades y controles de seguridad establecidos en la Autoridad Portuaria de Melilla y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de protección de datos de carácter personal y seguridad. Es el encargado de impulsar la implementación de la presente Política de Seguridad.

El Comité de Seguridad estará compuesto por los siguientes miembros:

a) Presidente: Director Autoridad Portuaria de Melilla
b) Secretaría: Técnico de Sistemas de Información y Comunicaciones
c) Vocalía: Jefe de División de Seguridad
c) Vocalía: Técnico de Sistemas de Información y Comunicaciones
d) Vocalía: Jefe División Sistemas de Información y Comunicaciones

El Comité de Seguridad, se reunirá con carácter ordinario, al menos una vez cada seis meses, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

El Responsable de Seguridad levantará actas de las reuniones del Comité de Seguridad. A las sesiones del Comité de Seguridad podrán asistir en calidad de asesores las personas que en cada caso estime pertinentes su Presidente.

Las funciones del Comité de Seguridad son las siguientes:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.
- Aprobar la normativa de seguridad de la información (security standards y security procedures).
- 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 respecto de ellos.
- 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.
- 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 diferentes 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.
- Asesorar de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:
  - Grupos de trabajo especializados internos, externos o mixtos.
  - Asesoría externa.
  - Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias.

7 ROLES: FUNCIONES Y RESPONSABILIDADES

7.1 Responsables de la información

- Serán personas con alto cargo en la dirección de la organización y pertenecientes al comité directivo del mismo. Este cargo 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 integridad.

- Esta responsabilidad recaerá en el titular del órgano o unidad administrativa que gestione cada procedimiento administrativo, pudiendo una misma persona acumular las responsabilidades de la información de todos los procedimientos que gestiones.

- Son los responsables, junto con los Responsables de los Servicios, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea.

7.2 Responsable de los Servicios

- Responsable de clasificar y determinar los niveles de seguridad de los servicios en cada dimensión de seguridad dentro del marco establecido en el Anexo I del ENS y en cada una de las dimensiones de seguridad conocidas y aplicables (disponibilidad, autenticidad, trazabilidad, confidencialidad e integridad), dentro del marco establecido en el Anexo I del ENS.

- Son los encargados, junto a los Responsables de la Información y contando con la participación y asesoramiento del Responsable de Seguridad de la Información y de los Responsables de los Sistemas de Información, de realizar los preceptivos análisis de riesgos, y de seleccionar las salvaguardas a implantar.

- Son los responsables, junto con los Responsables de la Información, de aceptar los riesgos residuales calculados en el análisis de riesgos, y de realizar su seguimiento y control, sin perjuicio de la posibilidad de delegar esta tarea. Esta responsabilidad recaerá en el titular del órgano que gestione cada servicio, independientemente de que exista un único responsable de los Servicios.

- Coordinar la interacción con otros organismos especializados.

- Promover las actividades de concienciación y formación en materia de seguridad en su ámbito de responsabilidad, siguiendo las directrices del Comité de Seguridad.

- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad.

- Elaborar Planes de mejora de la seguridad. Elaborar planes de concienciación y formación. Elaborar planes de continuidad de negocio y sistemas.

- Elaboración y Supervisión del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación y cambios.

- El responsable del servicio puede **acordar** la suspensión del manejo de una cierta información o la prestación de un cierto servicio, si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información, Responsable de Seguridad y Responsable de Sistemas, **antes** de ser ejecutada.

7.3 Responsable de la seguridad de la información

- Responsable de que los servicios y sistemas de información de la Autoridad Portuaria de Melilla se mantengan con el mayor grado de seguridad atendiendo a los principios de confidencialidad, integridad y disponibilidad.

- Supervisar el cumplimiento de la presente Política, de sus normas, procedimientos derivados y de la configuración de seguridad de los sistemas.

- Asesorar en materia de seguridad a los distintos responsables de seguridad y al Comité de Seguridad así como reportar el estado de la seguridad del sistema.

- Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por los Responsables de los Servicios y de la Información, siguiendo en todo momento lo exigido en el Anexo II del ENS, declarando la aplicabilidad de dichas medidas.

- Asesorar, en colaboración con los Responsables de los Sistemas, los Responsables de los Servicios y de la Información, en la realización del análisis y gestión de riesgos, elevando el informe resultante al Comité de Seguridad.

- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones.

- Responsable de la ejecución directa o delegada de las decisiones del Comité de Seguridad así como de la implementación de medidas de seguridad adicionales.

- En aquellos sistemas de información que por su complejidad, distribución, separación física de elementos o números de usuarios se necesitara de personal adicional para llevar a cabo las funciones del Responsable de Seguridad, el Responsable de Seguridad podrá designar cuantos Responsables de Seguridad Delegados considere necesarios, incluyendo los Responsables de Seguridad relativos a la LOPD. Los Responsables de Seguridad Delegados se harán cargo,

en su ámbito, de todas aquellas acciones que delegue el Responsable de Seguridad teniendo dependencias funcionales directas con él.

Respecto a la documentación, son funciones del Responsable de Seguridad:

1) Aprobar y proponer al Comité de Seguridad la documentación de seguridad de segundo nivel (Normativas y Procedimientos de Seguridad) de obligado cumplimiento.
2) Supervisar la documentación de tercer nivel (Procedimientos Técnicos de Seguridad) de obligado cumplimiento.
3) Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.
4) Elaborar las actas de las reuniones del Comité de Seguridad.
5) Documentación de seguridad del sistema.

7.4 Responsable del sistema de información

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

- Realizar ejercicios y pruebas sobre el procedimiento operativo de seguridad y los planes de continuidad existentes.

- Seguimiento del ciclo de vida de los sistemas: especificación, arquitectura, desarrollo, operación, cambios.

- En aquellos sistemas de información que por su complejidad, distribución, separación física de elementos o números de usuarios se necesitara de personal adicional para llevar a cabo las funciones del Responsable del Sistema, el Responsable del Sistema podrá designar cuantos Responsables del Sistema Delegados considere necesarios, incluyendo los Responsables del Sistema relativos a la LOPD. Los Responsables del Sistema Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema teniendo dependencias funcionales directas con él.

Respecto a la documentación, son funciones del Responsable de Sistemas:

1) Aprobar y proponer al Comité de Seguridad la documentación de sistemas (Normativas y Procedimientos de Sistemas).
2) Supervisar la documentación de tercer nivel (Procedimientos Técnicos de Seguridad) de obligado cumplimiento.
3) Mantener la documentación organizada y actualizada, gestionando los mecanismos de acceso a la misma.
4) Documentación de ciclo de vida de los sistemas.

7.5 Administrador de la seguridad del sistema (ASS)

Los Administradores de la seguridad del sistema en la Autoridad Portuaria de Melilla, coincidirán, por motivos de eficiencia y limitación de recursos, con los Responsables asignados a Seguridad y Sistemas. Las funciones que desempeñarán son las siguientes:

- 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, en particular, los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

- La aplicación de los Procedimientos Operativos de Seguridad.

- Aprobar y realizar los cambios en la configuración vigente del Sistema de Información, previa notificación al Responsable del Servicio.

- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente, así como 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 proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

- Informar al Responsable de Servicio 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.

8. PROCEDIMIENTOS DE DESIGNACIÓN

La creación del Comité de Seguridad, el nombramiento de sus integrantes y la designación de los Responsable identificados en esta política, será propuesto por la dirección del organismo y autorizada por el presidente de la Autoridad Portuaria de Melilla.

El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

9. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC 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 Comité de Seguridad y difundida para que la conozcan todas las partes afectadas.

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 página web del organismo: URL http://www.puertodemelilla.es/

10. DATOS DE CARÁCTER PERSONAL

Para el tratamiento de datos de carácter personal en los sistema de información se seguirá en todo momento lo desarrollado en el documento de seguridad y su documentación asociada conforme a lo exigido en el Título VIII de las medidas de seguridad en el tratamiento de datos de carácter personal del 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.

11. 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 repetirá regularmente, al menos una vez al año, elevando las conclusiones al Comité de Seguridad. Se realizará un análisis de riesgos de los sistemas de información en periodos inferiores a un año cuando:

1) Se modifique la información manejada.
2) Se modifiquen los servicios prestados.
3) Ocurran incidentes graves de seguridad.
4) Se reporten vulnerabilidades graves.

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

dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

12. FORMACIÓN Y CONCIENCIACIÓN

El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todo el personal de la Autoridad Portuaria de Melilla y a todas las actividades de acuerdo al principio de seguridad integral recogido en el artículo 5 del ENS. A estos efectos, la Autoridad Portuaria de Melilla, propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

El Comité de Seguridad aprobará una Política de formación y concienciación en el tratamiento seguro de la información con los siguientes objetivos:

- Formación sobre la protección de la información de datos de carácter personal, orientada a los responsables de los ficheros y hacia los usuarios con privilegios sobre los datos.
- Formación sobre los procedimientos desarrollados y los riesgos existentes.

13. OBLIGACIONES DEL PERSONAL

Todos los miembros de la Autoridad Portuaria de Melilla tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a todos.

El incumplimiento manifiesto de la Política de Seguridad de la Información o la normativa y procedimientos derivados de ésta, podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes.

14. TERCERAS PARTES

Cuando la Autoridad Portuaria de Melilla 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 TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Autoridad Portuaria de Melilla utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad 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.

La Autoridad Portuaria de Melilla podrá contar con empresas y organismos externos que ayuden a mejorar sus sistemas de seguridad, mediante la contratación de auditorías, asistencias técnicas o trabajos y desarrollos especializados.

15. ESTRUCTURA NORMATIVA

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles, de manera que cada documento de un nivel se fundamenta en los de nivel superior:

a) Primer nivel: Política de Seguridad de la Información.
b) Segundo nivel: Normativas y Procedimientos de Seguridad.
c) Tercer nivel: Procedimientos Técnicos de Seguridad.
d) Cuarto nivel: Informes, registros y evidencias electrónicas.

15.1 Primer nivel: Política de Seguridad

Documento de obligado cumplimiento por todo el personal, interno y externo, de la Autoridad Portuaria de Melilla, recogido en el presente documento y aprobada mediante Resolución de la Presidencia del organismo.

15.2 Segundo Nivel: Normativas y Procedimientos de Seguridad.

Documentos de obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente. La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Responsable de Servicio bajo la supervisión del Comité de Seguridad.

15.3 Tercer Nivel: Procedimientos Técnicos de Seguridad.

Documentos técnicos orientados a guiar las tareas a realizar, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos técnicos es el Responsable del Servicio. En caso de que los procedimientos afectaran a varios sistemas de información, serán elevados al Comité de Seguridad.

15.4 Cuarto Nivel: Informes, registros y evidencias electrónicas.

Documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que existan este tipo de documentos es del Responsable de Sistemas.

15.5 Otra documentación.

Se podrá seguir en todo momento los procedimientos STIC, las normas STIC, las instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400,500 y 600.