Política de

Seguridad de la Información

Puerto de Gijón

Aprobada en la sesión del Consejo de Administración de 19 de diciembre de 2025

www.puertogijon.gob.es
985 17 96 00

Edificio de Servicios Múltiples
El Musel, s/n - 33212 Gijón
Principado de Asturias. España

Puerto de Gijón
Autoridad Portuaria de Gijón

Índice

Este documento es interactivo.

Capítulo 1

Introducción

Este documento constituye la Política de Seguridad de la Información de la Autoridad Portuaria de Gijón, en adelante APG, en cumplimiento de lo previsto en el artículo 12 del Esquema Nacional de Seguridad, aprobado por Real Decreto 311/2022, de 3 de mayo, en adelante ENS, y de la medida de seguridad org.1 establecida en el Anexo II de dicho ENS.

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

La Política de Seguridad de la Información recoge la postura de la APG en cuanto a la seguridad de la información, la seguridad de los sistemas de información o ciberseguridad y establece los criterios generales que deben regir la actividad del Organismo en este ámbito.

La APG depende de los sistemas de información 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 último de la seguridad de la información es garantizar que la APG pueda cumplir con sus objetivos, desarrollar sus funciones y prestar los servicios que le competen y, con ello garantizar la calidad, confidencialidad, integridad, autenticidad y trazabilidad de la información y asegurar la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

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

La APG debe cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida de los sistemas TIC (Tecnologías de la Información y la Comunicación), 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 su coste deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos donde se traten datos personales, se adquieran servicios TIC o se presten servicios que afecten a los sistemas de información.

Capítulo 2

Alcance

Esta política se aplica a todos los sistemas de información de la APG, a todas las personas que conforman la organización y a los prestadores de servicios o proveedores de soluciones TIC de la APG. Específicamente, se aplica al sistema de información que da soporte a los servicios/información del negocio, al ejercicio de derechos y cumplimiento de deberes por medios electrónicos, y a la interacción por medios electrónicos con los ciudadanos, la Comunidad Portuaria y la Administración Pública. Con carácter general, esta Política será de obligado cumplimiento para toda persona que tenga acceso a sistemas de información de la APG, ya sean empleados o no.

Esta política también será de aplicación a los diferentes activos, tangibles e intangibles, muebles e inmuebles de la APG.

Capítulo 3

Misión de la APG. Objetivos de la política

La Autoridad Portuaria de Gijón es un organismo público con personalidad jurídica y patrimonio propios, así como plena capacidad de obrar, que está adscrito al Ministerio de Transportes y Movilidad Sostenible a través del organismo público Puertos del Estado.

De conformidad con lo previsto en el artículo 25 del Texto Refundido de la Ley de Puertos del Estado y de la Marina Mercante, aprobado por Real Decreto Legislativo 2/2011, de 5 de septiembre, en adelante TRLPEMM, corresponde a la APG el ejercicio de las siguientes competencias en la zona de servicio del puerto de Gijón, El Musel:

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.

Para el ejercicio de dichas competencias, la APG desarrolla las funciones previstas en el artículo 26 del TRLPEMM.

Los objetivos en materia de seguridad de la información que la APG pretende garantizar con la presente Política son:

a) Garantizar la confidencialidad, integridad, autenticidad de la información y la continuidad en la prestación de los servicios.

b) Implementar medidas de seguridad en función del riesgo.

c) Formar y concienciar a los integrantes de la APG respecto a la seguridad de la información.

d) Implementar medidas de seguridad que permitan la trazabilidad de los accesos y respetar, entre otros, el principio de mínimo privilegio, reforzando también el deber de confidencialidad de las personas usuarias en relación con la información que conocen en el desempeño de sus funciones.

e) Desplegar y controlar la seguridad física haciendo que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso, atendiendo a los riesgos detectados.

f) Establecer la seguridad en la gestión de las comunicaciones mediante los procedimientos necesarios, logrando que la información que se transmita a través de las redes de comunicaciones sea adecuadamente protegida.

g) Controlar la adquisición, desarrollo y mantenimiento de los sistemas de información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Controlar el cumplimiento de las medidas de seguridad en la prestación de los servicios, manteniendo el control en la adquisición e incorporación de nuevos componentes del sistema.

i) Gestionar los incidentes de seguridad para la correcta detección, contención, mitigación y resolución de estos, adoptando las medidas necesarias para que los mismos no vuelvan a reproducirse.

j) Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación en materia de protección de datos.

k) Supervisar de forma continuada el sistema de gestión de la seguridad, mejorando y corrigiendo las ineficiencias detectadas.

Capítulo 4

Principios rectores de la política

La presente Política se apoya en los siguientes principios rectores:

a) Alcance estratégico:

La seguridad de la información cuenta con el compromiso y el apoyo del Consejo de Administración, de la Presidencia y de la Dirección de la APG y debe contar con el compromiso y el apoyo de todos los niveles de la entidad y deberá coordinarse e integrarse con el resto de las iniciativas estratégicas de forma coherente.

b) Seguridad integral:

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas de información, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

c) Gestión de la seguridad basada en los riesgos:

La gestión de la seguridad basada en los riesgos identificados permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. Las medidas de seguridad se establecerán en función de los riesgos a los que esté sujeta la información y sus sistemas y serán proporcionales al riesgo que tratan, debiendo estar justificadas. Se tendrán también en cuenta los riesgos identificados en el tratamiento de datos personales.

d) Prevención, detección, respuesta y conservación:

La seguridad de la información debe estar orientada a la prevención, detección, respuesta y conservación con la implementación de acciones preventivas de incidentes, minimizando las vulnerabilidades detectadas, evitando la materialización de las amenazas y cuando estas se produzcan garantizando una conservación segura de la información y manteniendo disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

e) Existencia de líneas de defensa:

La estrategia de seguridad de la entidad se diseña e implementa en múltiples capas de seguridad, dispuestas 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.

f) Vigilancia continua y reevaluación periódica:

La entidad implementa medios para la detección y respuesta a actividades o comportamientos anómalos, junto con otros que permita una evaluación continuada del estado de seguridad de los activos. Existirá también un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evaluación de los riesgos y sistemas de protección. 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.

g) Seguridad por defecto y desde el diseño:

Los sistemas deben estar diseñados y configurados para garantizar la seguridad por defecto. Los sistemas proporcionarán la funcionalidad mínima necesaria para prestar el servicio para el que fueron diseñados.

h) Diferenciación de responsabilidades:

Las funciones del responsable de la seguridad y el responsable del sistema estarán diferenciadas. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

Capítulo 5

Cumplimiento normativo

Esta Política refuerza el compromiso de la APG con el cumplimiento normativo, y en particular, con las leyes y regulaciones que rigen la seguridad de la información, incluyendo la legislación en materia de protección de datos, y cualquier otra regulación específica del sector que impacte directamente en las operaciones de la Autoridad Portuaria de Gijón.

En el ámbito de la normativa de contratación aplicable al Organismo, la APG reconocerá y cumplirá con las disposiciones establecidas en los acuerdos 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.

La APG establecerá procedimientos para la revisión periódica de esta Política de Seguridad de la información, con el fin de asegurar que permanezca actualizada con respecto a los cambios en las leyes y normativas pertinentes. Además, se implementarán medidas de cumplimiento para verificar que las prácticas de seguridad de la información de la Autoridad Portuaria de Gijón estén alineadas con estos requisitos legales y regulatorios.

Las normas que constituyen el marco normativo aplicable en esta materia serán recogidas en un documento interno derivado como procedimiento de esta Política que deberá mantenerse actualizado por parte del Comité de Seguridad de la Información y accesible y disponible para todos los miembros de la Organización.

Capítulo 6

Organización de la seguridad

La seguridad de los sistemas de información comprometerá a todos los órganos de gobierno y gestión de la APG y todos los miembros de la organización, además por imperativo legal, la responsabilidad última del ENS y de la protección de datos se encuentra en el Director de la Autoridad Portuaria de Gijón.

Para garantizar el cumplimiento del ENS, la APG 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 (CSI).

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

- Comité de Seguridad de la Información
- Responsable de la Información
- Responsable del Servicio
- Responsable de Seguridad de la Información
- Responsable del Sistema
- Delegado de Protección de Datos
- Coordinador de Continuidad y Gestión de Crisis

Los roles, funciones y responsabilidades se detallan en la presente política en el ANEXO.

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 CSI desde el cual se evaluarán y se propondrán soluciones a los mismos, correspondiendo en todo caso la resolución a la Dirección de la Autoridad Portuaria.

El CSI es el órgano de la Autoridad Portuaria de Gijón que coordina al más alto nivel la Seguridad de la Información.

El CSI estará constituido por los siguientes miembros:

- Presidencia del CSI: Director de la APG
- Secretaría: Responsable de Seguridad de la Información
- Vocales: Responsable del Sistema, Delegado de Protección de Datos y Coordinador de Continuidad y Gestión de Crisis

Podrán ser invitados a participar en las sesiones del CSI, con voz, pero sin voto, y en función de las circunstancias, otros responsables de la Autoridad Portuaria de Gijón implicados en alguno de los aspectos relativos a la Seguridad de la Información.

Asimismo, 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 de la APG y en su caso al Consejo de Administración.

El Director de la APG ejercerá el rol de Responsable de la Información.

El Comité de Seguridad de la Información (CSI) desarrollará, de forma colegiada, las funciones y obligaciones asignadas al Responsable del Servicio, conforme a lo establecido en el Esquema Nacional de Seguridad.

La Autoridad Portuaria de Gijón designará formalmente mediante acuerdo de su Consejo de Administración a los miembros del CSI y a los siguientes responsables: Responsable de Seguridad de la Información, Delegado de Protección de Datos, Responsable de la Información, Responsable del servicio, Responsable del Sistema y Coordinador de Continuidad y Gestión de Crisis. De esa forma quedará formalmente constituido el CSI.

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.

Capítulo 7

Datos de carácter personal

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

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

El Delegado de Protección de Datos será miembro del CSI.

El análisis de riesgos de protección de datos será reevaluado de forma periódica, contando con el asesoramiento del Delegado de Protección de Datos. La implementación del plan de tratamiento del riesgo se coordinará con el del ENS, así como el resto de los procedimientos o normas de seguridad de la información, especialmente en lo relativo al control de los prestadores de servicios la respuesta a incidentes y/o brechas de datos personales.

Capítulo 8

Gestión de riesgos

Todos los sistemas de información sujetos a esta Política deberán realizar un análisis de riesgos que evalúe las amenazas y riesgos a los que están expuestos, incluyendo aquellos relacionados con la protección de datos personales.

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

Este análisis se repetirá en las siguientes circunstancias:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada o los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.
- Cuando se produzcan modificaciones en el análisis de riesgos de protección de datos o evaluaciones de impacto.

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.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Capítulo 9

Auditoría

Los sistemas de información de la Autoridad Portuaria de Gijón se someterán a una auditoría en base a los siguientes periodos y criterios:

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

Capítulo 10

Obligaciones del personal

Todos los miembros de la APG están obligados a conocer y cumplir con esta Política de Seguridad de la Información y las normas, procedimientos o guías que la desarrollen, siendo responsabilidad de la APG a través del CSI disponer y proporcionar los medios necesarios para que esta información llegue a todos los empleados afectados.

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

Las personas con responsabilidad en el uso, operación o administración de sistemas de información 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 perjuicio de otras implicaciones legales.

Capítulo 11

Terceras partes

Cuando la APG preste servicios o maneje información de otras entidades, se les informará sobre esta Política, sin perjuicio de respetar la normativa de aplicación. Además, se crearán canales de reporte y coordinación entre los respectivos Comités de Seguridad de la Información y se establecerán procedimientos conjuntos para la respuesta ante incidentes de seguridad.

Cuando la APG utilice servicios de terceros o comparta o ceda información a terceros, se les informará de esta Política, de la Normativa de Seguridad y de los Procedimientos de Seguridad aplicables a dichos servicios o información, sin perjuicio del cumplimiento de otras obligaciones legales. En la contratación de prestadores de servicios o adquisición de productos, incluyendo la adquisición de derechos de uso de activos en la nube, se tendrá en cuenta la obligación del adjudicatario de cumplir con el ENS.

Estos terceros deberán cumplir con las obligaciones establecidas en dicha normativa y podrán desarrollar sus propios procedimientos operativos para cumplirla, de modo que la APG pueda supervisarlos o solicitar evidencias el cumplimiento de estos, incluso auditorías de segunda o tercer parte. Se establecerán procedimientos específicos para el reporte y resolución de incidencias. Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política o el que específicamente se pueda exigir en el contrato.

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 la información/ servicios afectados antes del inicio de la contratación o, en su caso, de la adjudicación. El informe se trasladará el órgano de contratación de la APG que deberá decidir sobre la autorización de la continuación con la tramitación de la contratación, asumiendo los riesgos detectados.

Cuando la APG adquiera, desarrolle o implante un sistema de inteligencia artificial, además de cumplir con lo establecido en la normativa vigente en la materia, deberá contar con el informe del Responsable de Seguridad de la Información, que consultará al Responsable de la Información y del Servicio y, cuando sea necesario, al del Sistema, así como en todo caso al Delegado de Protección de Datos.

Capítulo 12

Gestión de incidentes de seguridad

La APG dispondrá de un procedimiento para la gestión ágil de los eventos e incidentes de seguridad que supongan una amenaza para la información y los servicios.

Este procedimiento se integrará con otros relacionados con los incidentes de seguridad de otras normas sectoriales como las de protección de datos personales u otras que afecten al Organismo para coordinar la respuesta desde los diferentes enfoques y comunicar a los diferentes organismos de control sin dilaciones indebidas y cuando sea preciso a las Fuerzas y Cuerpos de Seguridad del Estado o los Juzgados.

Capítulo 13

Desarrollo de la Política de Seguridad de la Información

Esta Política se desarrollará mediante la elaboración de otras políticas o normativas y procedimientos de seguridad que aborden aspectos específicos.

De este modo se conformará un sistema de gestión de la seguridad de la información cuya documentación se clasificará en cuatro niveles, estructurados jerárquicamente de la siguiente manera: Primer nivel: Política Seguridad de la Información; Segundo nivel: Normativas y Procedimientos de Seguridad; Tercer nivel: Procedimientos técnicos de Seguridad; Cuarto nivel: Registros y Evidencias Electrónicas.

Cada documento de un nivel inferior se basará y complementará 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.

a) 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 del Consejo de Administración de la APG.

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.

b) 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, garantizando así la correcta alineación con la Política de seguridad de la Información y los requisitos legales y técnicos pertinentes.

c) 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, supervisado por el Responsable de Seguridad de la Información.

d) 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.

Toda la documentación se encontrará a disposición de todo el personal de la organización que necesite conocerla y, en particular, el personal que utilice, opere o administre los sistemas de información y comunicaciones, la información albergada en dichos sistemas o los servicios prestados por la APG.

Esta documentación estará sujeta a un proceso de mejora continua, asegurando su actualización constante para adaptarse a los cambios en el panorama de riesgos, las normativas aplicables, las tecnologías emergentes y las lecciones aprendidas de incidentes de seguridad o auditorías.

Capítulo 14

Aprobación y entrada en vigor

Esta Política de Seguridad de la Información de la Autoridad Portuaria de Gijón fue aprobada por su Consejo de Administración en la sesión de 19 de diciembre de 2025.

Esta Política es de aplicación desde la fecha de su aprobación y hasta que en su caso sea modificada o reemplazada por una nueva Política.

El Comité de Seguridad de la Información de la Autoridad Portuaria de Gijón revisará la Política de forma ordinaria con carácter anual y de forma extraordinaria cuando se produzcan cambios que así lo aconsejen, elevando al Consejo de Administración de la APG las propuestas de modificación pertinentes.

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

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

Anexo

Roles: funciones y responsabilidades

Funciones del CSI

Son funciones del CSI:

1. Promover la mejora continua del sistema de gestión de la seguridad de la información.

2. Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.

3. Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.

4. Revisar regularmente la Política de Seguridad de la Información.

5. Aprobar la Normativa de Seguridad de la información.

6. Elaborar y aprobar los requisitos de formación, desde el punto de vista de seguridad de la información.

7. Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.

8. Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.

9. Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

10. Participar en la categorización de los sistemas y en el análisis de riesgos.

11. Revisar y aprobar los análisis de riesgos de los sistemas de información y los planes de acción para mitigarlos, así como dar seguimiento al cumplimiento de estos.

12. 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.

13. Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

14. 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 de información.

15. Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización.

16. Coordinación y supervisión del cumplimiento de la normativa la vigente en materia de seguridad de la información.

Responsable de la información

El ENS asigna al Responsable de la Información, como principal función, el establecimiento de los requisitos de la información tratada.

Responsable del Servicio

ENS asigna al Responsable del Servicio como función principal el establecimiento de los requisitos de los servicios prestados.

Responsable de Seguridad de la Información

El ENS atribuye al Responsable de la Seguridad determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios y supervisar la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportar sobre estas cuestiones.

Entre otras, desarrollará las siguientes funciones:

1. Mantener y velar por la seguridad de la información manejada y de los servicios prestados por los sistemas de información, de acuerdo con lo establecido en la Política de Seguridad de la Información.

2. Promover la formación y concienciación en materia de seguridad de la información. Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el CSI.

3. Elaborar y proponer para aprobación 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. Elaborará, junto al Responsable de Sistema, Planes de Mejora de la Seguridad, para su aprobación por el CSI.

4. Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.

5. Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.

6. 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-Ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información y su de Desarrollo.

7. Constituir el punto de contacto especializado para la coordinación con el CSIRT (Computer Security Incident Response Team) de referencia.

8. Notificar a la autoridad competente, a través del CSIRT (Computer Security Incident Response Team) de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.

9. 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.

10. Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

11. En caso de ocurrencia de incidentes de Seguridad de la Información, analizará y propondrá salvaguardas que prevengan incidentes similares en un futuro.

12. Convocará al CSI, recopilando la información pertinente.

13. 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.

14. Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema de Información.

15. Realizará el Análisis de Riesgos.

16. 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.

17. Facilitará al Responsable de Información y al Responsable 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.

18. Participará en la elaboración y aprobación, en el marco del CSI, de las Normativas de Seguridad de la Información.

19. Participará en la elaboración y aprobará los Procedimientos Operativos de Seguridad de la Información.

20. 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).

21. Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistema, que deberán ser aprobados por el CSI y probados periódicamente por el Responsable del Sistema.

22. Aprobará las directrices propuestas por el Responsable de Sistema para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.

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:

1. Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.

2. 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.

3. Llevar a cabo las funciones del administrador de la seguridad del sistema cuando no se disponga de uno:

a) La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información.

b) 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.

c) 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.

d) Aprobar los cambios en la configuración vigente del Sistema de Información.

e) Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

f) Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.

g) 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.

h) 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.

i) Informar al Responsable de Seguridad de la Información de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

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

Delegado de Protección de Datos

Las funciones del Delegado de Protección de Datos serán las previstas en la normativa de aplicación, principalmente las siguientes:

1. 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 de la normativa de protección de datos.

2. Supervisar el cumplimiento de las disposiciones de protección 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.

3. Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.

4. Cooperar con la autoridad de control.

5. Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa, y realizar consultas, en su caso, sobre cualquier otro asunto.

Coordinador de Continuidad y Gestión de Crisis

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:

1. Activación del Plan de Continuidad y Gestión de Crisis.

2. Bajo el criterio del Coordinador de Continuidad y Gestión de Crisis, podrá solicitar a diferentes perfiles según la naturaleza y nivel de la crisis.

3. Coordinación de las actividades de respuesta y recuperación.

4. Informar a los órganos de dirección sobre el estado y la evolución de la crisis.

5. Registro de la bitácora de actividad de la crisis, esta actividad podrá delegarse en otros miembros operativos.

6. Elaboración del informe final de crisis en colaboración con el resto de integrantes del CSI y equipo participante.

7. Cierre de la crisis.

8. Coordinación del programa del plan de pruebas de continuidad de negocio.

9. Coordinación de las actividades de auditoría de continuidad de negocio.

10. Coordinar los Planes de mejora.