GRUPO ADL

Política de seguridad de la información

ADL-PSI-1

Control del Documento

Título	Política de seguridad de la información
Documento	ADL-PSI-1
Fecha de creación	30/09/2025
Fecha modificación	14/11/2025
Versión	2.0

Registro de cambios del Documento

Versión	Causa del Cambio	Autor del Cambio	Fecha
1.0	Versión inicial	tiThink	30/09/2025
2.0	Modificación marco normativo	tiThink	14/11/2025

GRUPO ADL

Contenido

1 Aprobación y entrada en vigor

Texto aprobado el día 14 de Octubre de 2025 por la Dirección de Grupo ADL. Esta "Política de Seguridad de la Información", en adelante PSI, será efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política de seguridad de la Información que la sustituya.

2 Introducción

La asistencia y ayuda a domicilio es objetivo declarado de los agentes de las amenazas de ciberseguridad, que persiguen tanto la indisponibilidad de los sistemas atacados como el acceso a la información tratada, muy especialmente, la historia clínica y registros electrónicos asociados, así como los servicios asociados a sistemas y redes de comunicaciones. La ciudadanía, el usuario de los servicios debe ser considerado el centro de la seguridad de los sistemas de información asociados a los servicios asistenciales, focalizando medidas en los datos y en los derechos asociados, especialmente la seudonimización y medidas similares capaces de proteger la privacidad de aquellos frente a los ataques que pudieran presentarse.

Para hacer frente a 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 componentes del sistema de gestión del servicio de ayuda a domicilio de Grupo ADL deben aplicar las medidas adecuadas de seguridad de las exigidas por el Esquema Nacional de Seguridad (ENS), así como realizar un seguimiento continuo de los niveles de prestación de los servicios, monitorizar y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los Ciberincidentes para garantizar la continuidad de los servicios prestados.

Las organizaciones deben estar preparadas para soportar ataques al más alto nivel, que podrían poner en riesgo los servicios asistenciales críticos, que deberán ser coordinados con los procesos requeridos por ser servicios esenciales o infraestructuras críticas. Este esfuerzo debe provenir de todas las escalas de la pirámide asistencial, tanto en su nivel estratégico, pasando por las posiciones

operativas y alcanzando los niveles tácticos, interactuando con la cadena de suministro y proveedores. Las distintas organizaciones 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 la valoración de su coste deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en proyectos TIC. Debe requerirse un mayor esfuerzo si cabe a los proveedores, para que la seguridad forme parte de sus servicios y productos. Obviar este requerimiento es un riesgo que como servicio público esencial no se puede permitir y requiere de una estrategia de seguridad compartida y distribuida, en gran parte debido al aumento de la dependencia de éstos la prestación de los servicios asistenciales.

Por tanto, para el servicio que ofrece Grupo ADL, el objetivo prioritario de la Seguridad de la Información debe ser garantizar la calidad de la información y la prestación continuada de los servicios, actuando proactiva y preventivamente, supervisando la actividad diaria para detectar cualquier anomalía del sistema o incidente y reaccionando con presteza a los incidentes para recuperar los servicios lo antes posible, según lo establecido en el artículo 8 del ENS.

3 Medidas de prevención, detección, respuesta y recuperación

La transformación digital de los servicios asistenciales y la información asociada, implican la necesaria gestión de actividades de seguridad, que deben contemplar la proactividad, vigilancia y reactividad, por lo que se consideran todos los aspectos de prevención, detección y respuesta y recuperación, al objeto de minimizar al máximo los riesgos, de los sistemas de información que soportan y lograr que las amenazas sobre el los mismos no se materialicen o que, en el caso de hacerlo, tengan un impacto controlado y limitado, sin afectar gravemente a la información que maneja o a los servicios prestados.

Con carácter transversal se despliega una estrategia holística de seguridad que implica que el sistema de información dispone de una de protección basada en líneas de defensa, constituida por múltiples capas de seguridad, que interactúan y operan desde diferentes esferas.

Esta postura de seguridad solida permitirá que se desarrollen de forma continua y cíclica medidas de seguridad para aquellas situaciones y entornos que evolucionen de forma constante.

3.1 Prevención

Grupo ADL 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, debe implementar las medidas mínimas de seguridad, 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.

3.2 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 continua 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.

3.3 Respuesta

Se despliegan medidas de respuesta ante eventos que afecten a los servicios y/o información, permitiendo:

- Responder eficazmente a los incidentes de seguridad.
- Desarrollar una reacción adecuada frente a los incidentes, reduciendo al máximo la probabilidad de que el sistema sea comprometido en su conjunto.
- Designar un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros áreas, departamentos u organismos y en general en el sector sanitario.

- Establecer protocolos para el intercambio de información y coordinación necesaria, relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Las acciones de respuesta implicarán saber cómo responder, con que responder, quien responde y en qué momento se requiere cada acción.

4 Misión y objetivos

Son objetivos directos o misión clave, el proporcionar servicio para la promoción de la autonomía personal y gestión del servicio de ayuda a domicilio.

5 Principios básicos de seguridad

Los principios básicos, que se describen a continuación serán las directrices fundamentales de presentes en cualquier actividad del sistema de información.

- **Alcance estratégico**: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos, concierne a todos los miembros de la comunidad sanitaria, requiere estar coordinada e integrada con el resto de las iniciativas estratégicas de la estructura orgánica para conformar un todo coherente y eficaz.
- **Responsabilidad determinada**: Se determinará el Responsable de la Información, que determina los requisitos de seguridad de la información tratada; el Responsable del Servicio, que determina los requisitos de seguridad de los servicios prestados; el Responsable del Sistema, que tiene la responsabilidad sobre la implementación de seguridad y supervisión de la operativa del sistema y el Responsable de la Seguridad, que determina las decisiones para satisfacer los requisitos de seguridad y supervisará las medidas implantadas.
- **Seguridad integral**: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, 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.

- **Gestión de Riesgos**: La gestión de riesgos 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 que esté sujeta la información y sus sistemas de tratamiento.
- **Proporcionalidad**: Las medidas adoptadas para gestionar los riesgos deberán estar justificadas y, ser proporcionales entre ellas y los riesgos.
- **Mejora continua**: Existirá un proceso de mejora continua para la revisión y actualización de las medidas de seguridad, de manera periódica, conforme a su eficacia y la evolución de los riesgos y sistemas de protección.
- **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.

6 Objetivos de seguridad de la información

Se establecen como objetivos de la seguridad de la información los siguientes:

- Garantizar la calidad y protección de la información y los servicios.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.
- Gestionar los activos de información, bajo un inventario, clasificación y asignación a un responsable.
- Implementar medidas de seguridad ligada a las personas, incluyendo los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y reduzca el riesgo derivado de un su uso indebido, logrando la plena concienciación.
- Desplegar y controlar la seguridad física logrando que los activos de información se encuentren en áreas seguras, protegidos por controles de acceso físicos adecuados a su nivel de criticidad y frente a amenazas físicas o ambientales.
- Establecer la seguridad en la gestión de comunicaciones y operaciones mediante los procedimientos necesarios logrando que la información que

sea transmita a través de redes de comunicaciones sea adecuadamente protegida, conforme a su nivel de sensibilidad y de criticidad.

- Limitar el acceso a los activos mediante controles de acceso a usuarios, procesos y servicios, por medio de mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo, asegurando la trazabilidad del acceso y auditando su uso.
- 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.
- Mantener el control y la seguridad en la adquisición e incorporación de nuevos componentes del sistema, asociado a nuevas tecnologías desplegadas en los servicios de soporte o en su caso, en los servicios de telemedicina e información electrónica.
- Gestionarlos incidentes de seguridad para la correcta identificación, registro y resolución de estos.
- Garantizar la prestación continuada de los servicios de acuerdo con las necesidades de nivel de cada servicio.
- Proteger la información personal, adoptando las medidas técnicas y organizativas en atención a los riesgos derivados del tratamiento conforme a la legislación de seguridad y privacidad.
- Mejorar los procesos de identidad digital de las personas implicadas en los procesos de ayuda a domicilio.
- Adoptar las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

7 Alcance

Esta PSI se aplicará a los sistemas de información de Grupo ADL que están relacionados con la prestación de los servicios de ayuda a domicilio y a todas las personas usuarias con acceso autorizado a los mismos, sean o no personal público y con independencia de la naturaleza de su relación jurídica, estando todos ellos sometidos a la obligación de conocer y cumplir esta PSI y su Normativa de Seguridad derivada, siendo responsabilidad del Comité de Seguridad disponer los recursos y medios necesarios para lograr el cumplimiento de la misma.

8 Marco normativo

Grupo ADL cuenta con sede en Aguilar de la Frontera, provincia de Córdoba, pero ofrece sus servicios a lo largo de toda España, por lo que el marco normativo aplicable será el de obligado cumplimiento normativo nacional (España). Actualmente, se contempla:

El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y su corrección de errores del 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 libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD o Reglamento General de Protección de Datos)

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD) a nivel español y la normativa o leyes de aplicación para los servicios que Grupo ADL ofrece.

La Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia, de conformidad con el 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 la libre circulación de esos datos.

Ley 1/2019, de 20 de febrero, de Secretos Empresariales.

Ley 10/2021, de 9 de julio, de trabajo a distancia.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).

9 Directrices del Sistema de Gestión de Seguridad de la Información

La estructuración, gestión y acceso de la información que forma parte de la seguridad del sistema, se somete a las premisas, directrices, principios y requisitos de seguridad descritos en esta PSI y en concreto a:

- La información y los servicios se calificarán en base a lo dispuesto por la normativa aplicable, niveles según el valor de la información, y su sensibilidad y confidencialidad que pudiera requerir, y los criterios aprobados.
- Se desarrollará un sistema de gestión de la seguridad documentado, conforme a los requisitos planteados en la normativa vigente, sometido a un proceso de aprobación formal, con actualización y aprobación periódica.
- La calificación, junto con las evaluaciones de riesgo que se realicen, modularán las medidas de seguridad que se deberán aplicar.
- Los criterios señalados tendrán en cuenta la incidencia en la capacidad de la organización para lograr sus objetivos, la protección de sus bienes, el cumplimiento de sus obligaciones de prestación de servicios, el respeto a la legalidad y los derechos de los ciudadanos.
- Se establecerán medidas de seguridad en las distintas capas que intervienen en el tratamiento de la información. Estas medidas serán de carácter organizativo, físico y lógico.
- El personal será capacitado e informado de sus deberes y obligaciones en materia de seguridad de la información.
- Las personas que manejen información, que no sea pública, tienen la obligación de mantener la confidencialidad y el secreto, obligación que subsiste luego del término del vínculo.

10 Organización de la seguridad de la información

10.1 Criterios utilizados

Conforme a lo establecido en Real Decreto 311/ 2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) y las pautas establecidas en las Guías CCN-STIC, la organización de la seguridad de los sistemas de información responde a los siguientes criterios:

- La seguridad de los sistemas de información compromete a todos los miembros de la organización.
- Se considerará organización, al conjunto total de entidades, o a la entidad unitaria, o a la parte de la entidad, que diseña, despliega, ejecuta y mantiene bajo el ciclo de mejora continua, el sistema completo requerido por esta PSI.
- Se designarán roles de seguridad, conforme a lo establecido en el artículo 11 del ENS, esto es, Responsable del Servicio, Responsable de la Información, Responsable de la Seguridad, Responsable del Sistema, entre otros.
- Los roles se considerarán bajo el principio general de diferenciación de responsabilidades y pleno respeto a la atribución de cada uno de los roles, por cuanto se precisarán mecanismos adecuados para su coordinación y en su caso, resolución de conflictos.
- La responsabilidad de la seguridad de los sistemas estará diferenciada de la responsabilidad sobre la explotación de los mismos sistemas. Se considerarán niveles operativos y niveles tácticos para diferenciar claramente las funciones y responsabilidades.
- Se establece una estructura organizativa, con carácter estratégico, para la toma de decisiones en materia de Seguridad de la Información, y que conllevará las funciones clave de alto nivel y que se coordinará con las funciones operativas de seguridad.
- Se permitirá en su caso la creación de órganos y subróganos, con funciones delegadas entre los que distribuir aquellas funciones estratégicas y organizativas y tácticas, que sus titulares consideren.
- La estructura orgánica de seguridad se construirá en torno al denominado Comité de Seguridad de la Información, que ostentará la función de dirección de la seguridad en la organización.
- La presidencia de dicho Comité será ejercida por una persona física con la asunción formal de la responsabilidad de los actos.

10.2 Modelo de gobernanza

La presente PSI implica un modelo de gobernanza centralizado considerando las necesidades que presenta el servicio asistencial, por cuando se requieren una serie de servicios periféricos territorialmente desplegados.

La estructura organizativa de la seguridad contemplará una asignación clara de facultades y competencias en todos los niveles y la separación de las funciones detalladas en esta PSI y en el ENS. El necesario despliegue de estos servicios periféricos implica considerar responsabilidades y roles que han de ser asignados localmente y que implican puntos locales de seguridad. Todas las competencias se definirán en un organigrama que incluirá las líneas jerárquicas.

10.3 Funciones y responsabilidades

En el marco del ENS, los roles y órganos de la Seguridad de la Información, serán desplegados de manera estratégica en todos los niveles jerárquicos, considerando el más alto nivel de dirección y administración, y desplegando la estructura a niveles operativos o intermedios, incluyéndose secretarias o direcciones-subdirecciones y cuando existieran servicios o centros con nivel operativo, así como a niveles tácticos, asociados a servicios, áreas, departamentos y/o gerencias asistenciales o centros.

A tales efectos, los citados procederán a la designación de los responsables descritos y procederán a revisar sus nombramientos cada dos años o cuando su puesto quedara vacante.

Los distintos responsables, asumirán las funciones correspondientes a cada rol, en relación con la:

a) Gestión de la Seguridad de la Información.
b) Gestión de la seguridad operativa: medidas técnicas y tácticas y procedimientos.
c) Gestión de riesgos de seguridad de la información.
d) Gestión de incidentes de seguridad de la información y resiliencia del sistema.
e) Gestión de la mejora continua.
f) Gestión de la sensibilización y capacitación.

Se considerarán en todos ellos los siguientes roles, cuyas funciones se adecuarán a los niveles jerárquicos correspondientes

10.3.1 Responsable de la Información y Responsable del Servicio

Como Responsable del servicio, determina los requisitos (de seguridad) de los servicios prestados. Podrá considerarse a una persona física o a un órgano colegiado.

Como Responsable de la Información, determina los requisitos (de seguridad) de la información tratada. Podrá considerarse a una persona física o a un órgano colegiado.

La función del Responsable de la Información y Responsable del Servicio puede recaer en la misma persona o en un órgano colegiado al efecto.

Serán funciones del Responsable de la Información y del Responsable del Servicio:

- Determinar la valoración de la información y/o servicios conforme los criterios establecidos en la normativa en vigor.
- Determinar los requisitos de seguridad de la información y/o servicios.
- Dictaminar sobre los derechos de acceso a la información y los servicios.
- Aceptar los niveles de riesgo residual que afectan a la información y los servicios.
- Poner en comunicación del Responsable de la Seguridad cualquier variación respecto a la Información y los Servicios de los que es responsable, especialmente la incorporación de nuevos Servicios o Información a su cargo.
- En el caso de los servicios, determinar el impacto de una indisponibilidad de estos servicios en las actividades de los servicios sanitarios.

10.3.2 Responsable de Seguridad

Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. Por tanto, son funciones derivadas de este rol, aquellas relacionadas con el liderazgo de la seguridad y aquellas relacionadas con las operaciones de seguridad.

Será distinto del Responsable del Sistema, no debiendo existir dependencia jerárquica entre ambos. Excepcionalmente podrá ser autorizado por el máximo órgano de seguridad, que, en ausencia de recursos, obligue a que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, siempre que se desplieguen medidas compensatorias para garantizar la diferenciación de responsabilidades.

El Responsable de la Seguridad no podrá ser un órgano de gobierno y no deberá tener ninguna responsabilidad sobre la prestación de los servicios TIC.

Serán funciones del Responsable de la Seguridad:

- Desarrollar las funciones de supervisión de la seguridad, en colaboración con el Responsable del Sistema.
- Dirigir la Oficina de Seguridad Técnica y remitir reportes al Comité de Seguridad TIC.
- Determinar las decisiones y acciones necesarias, para cumplir con los requisitos de seguridad de la información y los servicios.
- Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los Servicios prestados por los sistemas de información.
- Promover la formación y concienciación en materia de seguridad de la información.
- Designar responsables de la ejecución de los procesos de análisis de riesgos, desarrollar, documentar y aprobar formalmente la Declaración de Aplicabilidad, identificación de las medidas de seguridad necesarias, determinar las configuraciones de seguridad necesarias, y encargarse de que el personal responsable elabore la documentación del sistema y en su caso, custodiarlo debidamente.
- Considerar medidas adicionales a las requeridas por el ENS, o en su caso, reemplazar las requeridas por otras compensatorias, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados.
- Proporcionar asesoramiento para la determinación de la Valoración del Sistema, en colaboración con el Responsable del Sistema y/o Comité de Seguridad de la Información de la Información, y determinar la categoría de seguridad correspondiente para el sistema.

- Participará en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad, procediendo a su validación.
- Gestionar las revisiones externas o internas del sistema, presentando las conclusiones a los órganos correspondientes y al Responsable del Sistema.
- Gestionar los procesos de certificación.
- Elevar al Comité de Seguridad la aprobación de cambios y otros requisitos del sistema.
- Aprobar los procedimientos de seguridad que forman parte del Mapa Normativo (y no son competencia expresa de otros roles) y poner en conocimiento de los órganos de seguridad [Comité], de las modificaciones que se hayan realizado a lo largo del periodo en curso.
- Coordinar con el CSIRT y/o la Autoridad de Control correspondiente, cualquier "incidente" que tenga un impacto significativo en la prestación de sus servicios. En su caso, notificar a las personas destinatarios de los servicios sanitarios, información relacionada con el incidente, las medidas o soluciones frente a la ciberamenaza o cualquier información que se considere relevante.

Las anteriores funciones se modulan en roles designados en posiciones intermedias o inferiores de la estructura orgánica de salud.

Para el desarrollo de las funciones se pueden considerar un único Responsable de la Seguridad o varios, diferenciando claramente sus funciones y responsabilidades y el ámbito de actuación asignado. El Responsable de la Seguridad podrá delegar funciones en otras personas u órganos o entidades, pero no podrá delegar la responsabilidad de las siguientes:

- Funciones relacionadas con la normativa, identificación de las tendencias de seguridad seguidas por el sistema, y el seguimiento de la mejora y eficiencia del sistema.
- Supervisión y conformidad del sistema.
- Operativas de la seguridad del sistema.
    - Medidas de seguridad generales, salvo su aprobación.

    - Medidas de seguridad complementarias o fuentes añadidas, salvo su aprobación.
    - Medidas compensatorias o complementarias, salvo su aprobación.
- Ejecución del análisis de riesgos y desarrollo de propuesta de tratamiento de riesgos.
- Procedimientos operativos de seguridad.
- Propuestas de formaciones y acciones de sensibilización.
- Desarrollo de análisis de continuidad y propuestas de estrategias de resiliencia.
- Análisis del ciclo de vida de los componentes del sistema.
- Análisis de seguridad o auditorias del sistema técnico mediante análisis de caja blanca, gris o negra.

Además de las características y funciones señaladas, el Responsable de la Seguridad, en los aspectos relativos a la seguridad lógica que le correspondan, podrá integrar las funciones de seguridad de otros roles que pudieran ser necesarios por imperativo legal o por normativas sectoriales o particulares que contemplen la asunción de obligaciones específicas para los órganos, organismos o unidades del sector público implicados en los servicios sanitarios, pudiendo asumir, asimismo, las funciones de coordinación con el CSIRT correspondiente.

10.3.3 Responsable del Sistema

Se encargará de implementar la seguridad en el sistema y supervisar la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad. Podrá desarrollar por sí mismo o mediante el apoyo en terceros, la ejecución de sus tareas y funciones concretas.

Podrá apoyarse en áreas o servicios propios o de terceros con funciones en ciberseguridad para el desarrollo de funciones específicas proactivas y tácticas, como vigilancia, monitorización y respuesta.

Serán funciones del Responsable del Sistema:

- Desarrollar las funciones operativas de la seguridad, en colaboración con el Responsable de la Seguridad.
- Dirigir el Centro de Operaciones de Seguridad y cuando se designará, del Centro de Gestión de Incidentes.

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluidas sus especificaciones, instalación y verificación de su correcto funcionamiento y elaborando los procedimientos operativos necesarios.
- Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Implantar las medidas técnicas de seguridad aprobadas en los planes de tratamiento de riesgos.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Colaborar en el desarrollo de la normativa para el uso de las tecnologías de la información y las comunicaciones.
- Colaborar en la redacción de planes de contingencia, para lo cual se realizarán las comprobaciones necesarias para comprobar su eficacia.
- Detener el acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
- Proporcionar asesoramiento para la determinación de la Categoría del Sistema, en colaboración con el Responsable de la Seguridad y/o Comité de Seguridad de la Información de la Información.
- Garantizará que los dispositivos que abandonen las instalaciones mantienen la seguridad necesaria conforme a las necesidades de la información que manejan.
- Analizar las conclusiones elevadas por el Responsable de la Seguridad de las auditorías, revisiones internas y autoevaluaciones realizadas y proponer medidas.

Además, para llevar a cabo, en su caso, las funciones del administrador de la seguridad del sistema:

- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.
- La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con 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 componentes, su mantenimiento, 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 proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.
- Informar al Responsable de la Seguridad 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.

Cuando la complejidad del sistema lo justifique, el Responsable del Sistema podrá designar los responsables de sistema delegados que considere necesarios, que tendrán dependencia funcional directa de aquél y serán responsables en su ámbito de todas aquellas acciones que les delegue el mismo. De igual modo, también podrá delegar en otro/s funciones concretas de las responsabilidades que se le atribuyen tales como:

- Medidas de identificación, autenticación y asignación.
- Monitorización y seguimiento actividades.
- Ciberinteligencia y vigilancia activa.
- Interconexiones y seguimiento de autorizaciones de flujos.
- Gestión de bastionados.
- Parcheados y actualizaciones no criticas.
- Cambios menores o preautorizados.
- Entradas en producción de servicios no críticos y/o previamente desplegados en entornos de preproducción.

Podrá contar con servicios o áreas con funciones en ciberseguridad, monitorización vigilancia y detección y respuesta del sistema ante cualquier ataque.

10.3.4 Delegado de protección de datos

Con la designación de un delegado de protección de datos, Grupo ADL podrá recabar del mismo el asesoramiento cuando la seguridad afecte al tratamiento de datos de carácter personal. El delegado de protección de datos podrá realizar también funciones de supervisión conforme a lo regulado en el RGPD. Podrá ser convocado al Comité de Seguridad de la Información cuando sea preciso por motivo del tratamiento de asuntos que afecten a datos personales y participará con voz, pero sin voto.

10.3.5 Comité de seguridad TIC (COMSEGTIC)

Este comité será considerado el más alto órgano especializado integrado por aquellas personas con responsabilidad en la toma de decisión en seguridad de la información y aquellas que sean designadas por representación de las distintas entidades y unidades, y se encargará de la coordinación de los restantes órganos, que serán dependientes de este y al que reportarán en base a la distribución de funciones y tareas que se haga.

- Presidencia
- Vocales:
    - Miembros permanentes:
        - Secretario/a del COMSEGTIC: Secretario General o delegado
        - Responsable del Sistema (RSIS)
        - Responsable de la Seguridad de la Información (RSEG)
        - Representantes de Información y Servicios considerados a efectos de alto nivel.
        - Asesores que se consideren oportunos para los temas en cuestión, pudiendo incluso acudir un representante del Centro Criptológico Nacional (CCN), con voz, pero sin voto.
        - Representantes de órganos de seguridad inferiores constituidos a efectos de lo descrito en esta PSI.
        - Cuando existieran, representantes de la Oficina de seguridad, área o servicio de ciberseguridad y en su caso, órgano de auditoría interna.
        - El Delegado de Protección de datos, con voz, pero sin voto.
    - Miembros no permanentes:

- Podrá invocar la presencia en sus reuniones tanto de otros representantes de las diferentes entidades públicas del sector salud y/o servicios sanitarios, así como especialistas externos, de los sectores público, privado y/o medicina y salud y/o ciberseguridad, cuya presencia, por razón de su experiencia o vinculación con los asuntos a tratar, sea necesaria o aconsejable.

Los Representantes de la Información y los Servicios serán convocados por la presidencia en función de los asuntos a tratar, en representación de los distintos ámbitos o áreas/departamento. Cada área/departamento estará representada por un vocal con voto, sin perjuicio de que acudan varios representantes de esta.

El Secretario/a del Comité realizará las convocatorias y 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 o a petición de cualquiera de sus miembros.

Se considerarán órganos similares al descrito, para la integración de roles designados en posiciones jerárquicas inferiores, tales como áreas, departamentos y gerencias. Estos órganos se denominarán con el término "Sub" para identificar la dependencia directa del mismo, al órgano inmediatamente superior.

El órgano superior detallará las funciones delegadas o encargadas al órgano inferior. Sin perjuicio de aquellas otras funciones que deban ser acometidas por el mismo, son funciones esenciales del Comité de Seguridad TIC;

Atribuciones del Comité de Seguridad TIC:

- Para la coordinación en la seguridad de la información:
    a. Elaborar la estrategia global de seguridad de la información de la prestación sanitaria en el ámbito territorial correspondiente.
    b. Desarrollar un marco común normativo, organizativo y colaborativo de seguridad de la información.
    c. Aprobar un marco común de indicadores, métricas y analítica de datos de seguridad de la información.
    d. Adoptar y realizar un seguimiento en relación con la efectividad de los objetivos de seguridad de la información.

e. La mejora continua del proceso de seguridad.
f. Promover la elaboración del informe anual del estado de seguridad de los sistemas TIC, asociados a la prestación sanitaria.
g. Priorizar los recursos en materia de seguridad y promover la mejora continua de la seguridad de la información.
h. Intercambiar experiencias, conocimiento, herramientas y casos de éxito de seguridad. i. Promover la integración con otros marcos de gobernanza de seguridad.
i. Coordinar a los diferentes órganos y roles de seguridad de la información.
j. Resolver conflictos de responsabilidad entre diferentes órganos y/o responsables y/o áreas/ departamentos.

- Para el desarrollo de la normativa en materia de seguridad.
  a. Propuesta y mejora continua e innovación de la normativa de seguridad.
  b. Aprobar la Normativa de Uso de Medios electrónicos para todo el personal del ámbito sanitario.
  c. Integración en la normativa de las buenas prácticas en seguridad de la información, de ámbito nacional y europeo.
- Para la gestión de riesgos de seguridad de la información.
  a. Adoptar un marco común de gestión de riesgos para los sistemas TIC asociados a los servicios de prestación sanitaria.
  b. Definir los requisitos, niveles mínimos y criterios comunes para la Categorización y Declaración de Aplicabilidad en la prestación sanitaria.
  c. Seguimiento de planes de tratamiento de riesgos y planes de acción.
  d. Aprobación de informes relacionados con los niveles de riesgos de servicios y componentes implicados en la prestación sanitaria.
- Para la conformidad de la seguridad de la información
  a. Promover la constitución de una unidad específica que asuma las funciones de auditoría y en su caso, promover la acreditación como Organismo de Auditoria Técnico.
  b. Aprobar los planes de revisión y auditoria de seguridad.
  c. Estar permanentemente informado de la normativa que regula la Conformidad con el ENS, incluyendo sus normas de acreditación,

certificación, guías, manuales, procedimientos e instrucciones técnicas y perfiles de cumplimiento específicos aplicables.

d. Conocer la relación de Entidades de Certificación acreditadas y organizaciones, públicas y privadas, certificadas.

- Para la formación de la seguridad de la información.
  a. Aprobar el plan anual de formación y sensibilización de usuarios implicados en la prestación sanitaria.
  b. Dotar de recursos los planes de formación y concienciación en materia de seguridad y protección de datos personales.
- Para la gestión de incidentes y eventos de seguridad de la información
  a. Promover una postura de seguridad sólida, con base en la ciberinteligencia de amenazas.
  b. Mantenerse permanente informado de la gestión de incidentes.
  c. Liderar los procesos de notificación de incidentes y declaración de escenarios de contingencia en la prestación sanitaria.
  d. Coordinar las actuaciones ante incidentes críticos para la prestación sanitaria con las autoridades competentes.
  e. Mantener el flujo e l intercambio de información con otros órganos y organismos, CSIRT de referencia y autoridades competentes.
- Para la monitorización y vigilancia de seguridad de la información.
  a. Potenciar las acciones de vigilancia en las operaciones del sistema, monitorizando la red, los servicios y la infraestructura.
  b. Promover servicios de alerta temprana y gestión de vulnerabilidades.

El comité de seguridad se regirá por lo dispuesto en esta PSI y en la norma interna que regulará su funcionamiento.

Para desplegar las funciones declaradas en la presente, se podrá apoyar en el rol del Responsable de la Seguridad, en el Centro de Operaciones de Seguridad y en Unidades operativas, por ejemplo, de gestión de eventos o incidentes de seguridad.

El comité también podrá considerar la creación de un otros sub-comités, órganos o grupos de trabajo en los que delegue funciones, debiendo quedar estas adecuadamente documentadas.

Periodicidad de las reuniones y adopción de acuerdos:

- Durante el desarrollo de acciones estratégicas y operativas de seguridad que requieren seguimiento para evaluar su desarrollo, el Comité de Seguridad TIC se reunirá, al menos, una vez al trimestre.
- Para el desarrollo de funciones ordinarias y de mejora continua, se reunirá, al menos, dos veces al año con carácter semestral, sin perjuicio de que, en atención a las necesidades derivadas del cumplimiento de sus fines y atribuciones, requiera de una mayor frecuencia en las reuniones.
- En cualquier caso, las reuniones se convocarán por su Presidencia, a través del Secretario, a su iniciativa o por mayoría de sus miembros permanentes.
- Las decisiones se adoptarán por consenso de los miembros permanentes.

10.3.6 Otros roles o responsabilidades

Podría considerarse otros roles de seguridad que pudieran ser necesarios por imperativo legal, y normas particulares que detallen obligaciones específicas a Grupo ADL.

10.4 Procedimiento de designación

El responsable de la información, responsable de servicio, responsable de seguridad de la información y el responsable y administrador del sistema serán nombrados por Grupo ADL a propuesta del Comité de Seguridad TIC, teniendo la última palabra el/los representante/s de la dirección que se encuentren en el comité. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante. Los motivos para renovar o designar una nueva persona serán los siguientes:

- Habilidades y destrezas actuales en la empresa
- Cargo actual que desempeña y su adecuación al puesto en el comité
- Continuidad como empleado en la empresa
- Disponibilidad para desempeñar el cargo
- Decisión del comité y como última palabra, decisión de la dirección de la empresa

El DPD al ser un perfil externo, al igual que en los otros perfiles, será nombrado por Grupo ADL a propuesta del Comité de Seguridad TIC y su nombramiento se revisará cada año o cuando el puesto quede vacante. La diferencia en los motivos

será que, en este caso, no aplican los posibles cambios dentro de la organización sino a decisiones respecto al contrato con la empresa externa o decisiones de la propia empresa externa que aporta el perfil de DPD.

11 Datos personales

Grupo ADL, como responsable del tratamiento, trata los datos personales de acuerdo con los principios y obligaciones recogidos tanto en el Reglamento 679/2016, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la Protección de las Personas Físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos-RGPD-) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, respetando, en todo caso, el derecho fundamental a la protección de datos personales, la intimidad y el resto de los derechos fundamentales reconocidos tanto en la legislación y tratados internacionales como en la Constitución vigente.

El responsable del tratamiento pone a disposición de las personas afectadas información pormenorizada sobre el tratamiento de sus datos personales y sobre como ejercitar sus derechos de acceso, rectificación, supresión y, cuando ello sea posible, oposición, limitación y portabilidad.

Además, el responsable del tratamiento ha designado y registrado ante la autoridad de control un Delegado de Protección de Datos que, de forma independiente y especializada, le asesora en el cumplimiento de las obligaciones de la normativa de protección de datos, supervisa sus actuaciones, responde a las consultas de los interesados y a las de la Agencia Española de Protección de Datos

12 Obligaciones del personal

Todas las personas que utilicen la información y/o servicios y/o sistemas de tratamiento sometidos a esta PSI, tienen la obligación de conocer y respetar su contenido y en el marco normativo de desarrollo que se apruebe por cumplimiento directo de la misma.

Todo el personal de Grupo ADL, comprendido dentro del ámbito del ENS, atenderá a una o varias sesiones de concienciación en materia de seguridad y protección de datos, al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal, en particular al 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.

13 Gestión de riesgos

Todos los sistemas afectados por la presente PSI están sujetos a la gestión de riesgos con el objetivo de evaluar las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Al menos una vez al año.
- Cuando cambien la información y/o los servicios manejados de manera significativa.
- Cuando ocurra un incidente grave de seguridad o se detecten vulnerabilidades graves.

El Responsable de la Seguridad será el encargado de que se realice el análisis de riesgos, así como de identificar carencias y debilidades y ponerlas en conocimiento del Comité de Seguridad de la Información.

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.

El proceso de gestión de riesgos comprenderá las siguientes fases:

- Categorización de los sistemas.
- Análisis de riesgos.

- El Comité de Seguridad de la Información procederá a la selección de medidas de seguridad a aplicar que deberán de ser proporcionales a los riesgos y estar justificadas.

En particular, para realizar el análisis de riesgos, con carácter general, se empleará una metodología reconocido prestigio en el ámbito de la seguridad de la información para el análisis y gestión de riesgos

14 Notificación de incidentes

De conformidad con lo dispuesto en el artículo 36 del ENS, como titular de sistemas de información bajo el ámbito de aplicación del mismo, dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33 del ENS, la Instrucción Técnica de Seguridad correspondiente y, en su caso, cuando se trate de un operador de servicios esenciales bajo las prescripciones establecidas por la normativa sectorial vigente.

Igualmente dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Se desplegarán las medidas y mecanismos necesarios para notificar al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados en relación con la categorización de sistemas.

Se interactuará con los CERT-CSIRT correspondientes y se mantendrán todas las medidas requeridas por los equipos de respuesta de autoridades.

15 Desarrollo de la política de seguridad de la información

La presente PSI será complementada por medio de diversa normativa y recomendaciones de seguridad (normativas y procedimientos de seguridad, procedimientos técnicos de seguridad, informes, registros y evidencias electrónicas).

Corresponde al Comité de Seguridad de la Información su revisión anual y/o mantenimiento, proponiendo, en caso de que sea necesario mejoras a la misma.

El cuerpo normativo sobre seguridad de la información se desarrollará en tres niveles por ámbito de aplicación, nivel de detalle técnico y obligatoriedad de cumplimiento, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

- Primer nivel normativo: constituido por la presente PSI, la Normativa Interna del Uso de los Medios Electrónicos y las directrices generales de seguridad aplicables a los organismos, áreas o departamentos a los que sea de aplicación dichos documentos.
- Segundo nivel normativo: constituido por las normas de seguridad derivadas de las anteriores.
- Tercer nivel normativo: constituido por procedimientos, guías e instrucciones técnicas. Son documentos que, cumpliendo con lo expuesto en la PSI, determinan las acciones o tareas a realizar en el desempeño de un proceso.

Corresponde al órgano superior de Grupo ADL, la aprobación de la PSI y la Normativa Interna del Uso de los Medios Electrónicos, siendo el Comité de Seguridad de la Información el órgano responsable de la aprobación de los restantes documentos, siendo también responsable de su difusión para que la conozcan las partes afectadas.

Del mismo modo, la presente PSI complementa la Política de Privacidad en materia de protección de datos.

La normativa de seguridad y, muy especialmente, la PSI y la Normativa Interna del Uso de los Medios Electrónicos, será conocida y estará a disposición de todos los miembros, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

Estará disponible para su consulta en servicios publicados con o sin acceso libre, en soporte papel, y formará parte de los planes de formación del personal y usuarios con acceso al sistema de información

16 Terceras partes

Cuando se preste servicios a otros organismos o maneje información de otros organismos, se les hará participe de esta PSI.

Se establecerán canales para el reporte y la coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o se ceda información a terceros, se les hará participe de esta PSI 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 PSI.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Si bien se deberá atender a las especialidades del sector y específicamente la dependencia o exclusividad que pudiera presentarse, en caso de no disponer de proveedores que dispongan de las correspondientes conformidades requeridas en ENS, deberán requerirse medidas de seguridad acordes a la valoración del riesgo tanto para la información como para el servicio que vaya a prestarse, requiriendo informe del Responsable de la Seguridad que precise los riesgos en

que se incurre y la forma de tratarlos. Dicho informe deberá ser aprobado por el Responsable de la información y Responsable del Servicio, con carácter previo al inicio de la relación con la tercera parte o en su caso, elevarse al Comité de Seguridad quien deberá valorar la motivación presentada y aprobar en su caso la contratación.

17 Mejora continua

La gestión de la seguridad de la información es un proceso sujeto a permanente actualización. Los cambios en la organización, las amenazas, las tecnologías y/o la legislación son un ejemplo en los que es necesaria una mejora continua de los sistemas.

Por ello, es necesario implantar un proceso permanente que comportará, entre otras acciones:

a) Revisión de la Política de Seguridad de la Información.
b) Revisión de los servicios e información y su categorización. CCN-STIC-891 Anexo II. Política de Seguridad para SALUD Centro Criptológico Nacional 36
c) Ejecución con periodicidad anual del análisis de riesgos.
d) Realización de auditorías internas o, cuando procedan, externas.
e) Revisión de las medidas de seguridad.
f) Revisión y actualización de las normas y procedimientos.

18 Desarrollo de la política de seguridad de la información

El cumplimiento de los objetivos marcados en esta PSI se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento del Esquema Nacional de Seguridad. Para su organización se ha definido una Norma para la Gestión de la Documentación, que establece las directrices para la organización, gestión y acceso. La revisión anual de la presente PSI corresponde al Comité de Seguridad de la Información proponiendo en caso de que sea necesario mejoras de esta, para su aprobación por parte del mismo órgano que la aprobó inicialmente.


GRUPO ADL