Guía de Seguridad de las TIC
CCN-STIC 891

Anexo II. Política de Seguridad para Salud
Prestación sanitaria a pacientes
(Atención Primaria y Atención Especializada)

Febrero 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.02.08 12:32:14 +01'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2023

Fecha de Edición: febrero de 2024

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. Aprobación y entrada en vigor

Texto aprobado el día __ de _____ de _____ por Resolución del [ÓRGANO CON COMPETENCIAS – "CONSEJERIA"] al que se encuentra adscrito o depende o a cuya resolución se adhiere de la/del [ENTIDAD/ORGANIZACIÓN/ORGANISMO].

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 sanitaria 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 sanitario de la/del [ENTIDAD/ORGANIZACIÓN/ORGANISMO] 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 pliegos de licitación para proyectos de 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 tan

importantes como la telemedicina o la necesaria gestión de la información en modo electrónico y procesamiento de datos al más alto nivel. Los proveedores del sector sanitario presentan características específicas que deben ser consideradas por esta PSI, especialmente la reducida presencia de competitividad y exclusividad, y la clara focalización como objetivo de interés para los ciberatacantes actuales en ellos, que ponen a los proveedores y a servicios asistenciales, en el centro de los ataques de ciberseguridad.

Por tanto, para la asistencia sanitaria, 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 de 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

Comprende las diversas medidas de prevención, que podrán incorporarse con el propósito de lograr la disuasión o a la reducción de la superficie de exposición, gestionando la materialización de las amenazas. Es necesario trabajar en un análisis de la exposición y riesgo del sistema, conocer tendencias en ataques del sector, analizar los Ciberincidentes en nuestro entorno y aprender del sector y de las lecciones extraídas en seguridad.

Además de incluir análisis de evoluciones y tendencias, se deben considerar las motivaciones de los atacantes y, los impactos potenciales, de manera que se pueda analizar y decidir claramente sobre qué medidas defensivas son requeridas por el sistema, y qué efectividad se espera.

Con carácter general, se establece el principio general de autorización y control de los sistemas, previo a su entrada en operación.

Deben considerarse los riesgos a los que está expuesto el sistema, tanto en el momento actual como aquellos otros que pudieran presentarse en el futuro. Se considera la necesidad de la revisión y evaluación continua y permanente de la seguridad del sistema y sus activos, permitiendo la mejora continua y la eficacia de las medidas de seguridad acordadas, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario. Obtener un análisis en profundidad de las amenazas, así como de las tácticas, técnicas y procedimientos de los principales ciberatacantes del sector sanitario, es fundamental para la preparación y resiliencia del sistema.

3.2 Detección

Se establecen controles de operación para los sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto en el artículo 10 del ENS (vigilancia continua y reevaluación periódica). Entre otras acciones se trata de identificar patrones en ataques a partir de los cuales se podrían desarrollar reglas lógicas del sistema para detectar indicadores específicos de actividades maliciosas o actores conocidos en el sector sanitario.

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.

3.4 Recuperación

Se establecen protocolos clave para garantizar la disponibilidad de los servicios y en su caso, la estrategia de gestión de los medios y técnicas necesarias que permitan garantizar la recuperación de los servicios más críticos. Las estrategias de contingencia pueden ser claves en la cadena de suministradores, por lo que podrá extenderse más allá del propio servicio.

4. Misión u objetivos

Son objetivos directos o misión clave, la gestión de servicios asistenciales básicos conforme a las funciones y competencias atribuidas por diferentes normas y, en concreto por el artículo 8 bis de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud. Es decir, el desarrollo de servicios asistenciales relativos a *prevención, diagnóstico, tratamiento y rehabilitación* que se realicen en centros sanitarios o sociosanitarios, cubiertos de forma completa por financiación pública [o participada].

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 la 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 sanitarios,
- 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 la/del [ENTIDAD/ORGANIZACIÓN/ORGANISMO] que están relacionados con la prestación de los servicios asistenciales sanitarios y que se encuentran dentro del ámbito de aplicación del Real Decreto 311/2022 de 3 mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), indicados en el artículo 8 bis de la Ley 16/2003, que incluyen las actividades asistenciales de prevención, diagnóstico, tratamiento y rehabilitación que se realicen en centros sanitarios y sociosanitarios, así como el transporte sanitario urgente, cubiertos de forma completa con financiación pública, todos ellos relacionados con el ejercicio de sus competencias 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 todo sellos 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

[NOTA: revisar – tener en cuenta normativa sectorial y/o autonómica, etc.]

[RECOMENDACIÓN: reducir al máximo este punto y detallar como y donde se puede consultar el marco normativo aplicable vigente. Se debería desplegar un proceso y documentar un procedimiento para identificar el marco normativo y su pertinente registro y actualización. Se puede publicar, por ejemplo, en la sede electrónica, portal de transparencia…]

La base normativa que afecta al desarrollo de las actividades y competencias de la organización y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por la siguiente legislación:

- Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

- Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual
- Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (enlace a https://www.boe.es/doue/2014/257/L00073-00114.pdf), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (reglamento eIDAS).

- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2013, de 27 de diciembre, de Impulso de la factura electrónica y creación del Registro electrónico de facturas en el sector público.
- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (archivo).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (Vigente en los apartados señalados en la Disposición Derogatoria Única de la Ley 11/2022, de 28 de junio).
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

- Ley 11/2022, de 28 de junio, General de Telecomunicaciones (según plazos entrada en vigor de Disposición de esta Ley).

[NOTA: completar con demás normativa que se aplique en el ámbito autonómico]

También forman parte del marco normativo la Política de firma electrónica de la/del [ENTIDAD/ORGANIZACIÓN/ORGANISMO].

También se consideran las restantes normas aplicables a los servicios bajo el objeto de aplicación del ENS, y comprendidos dentro del ámbito de aplicación de la presente PSI.

El mantenimiento del marco normativo será responsabilidad de cada organización, y se mantendrá en un Anexo, incluyéndose las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante la resolución de la Secretaría de Estado con competencias, y aprobadas por el correspondiente Ministerio, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el ENS.

Así mismo, se identificarán las guías de seguridad del CCN, referenciadas en el mencionado artículo, que se aplicarán en el cumplimiento de lo establecido en el ENS.

9. Directrices del sistema de gestión de la 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 para la organización de la Seguridad de la Información

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:

i. La seguridad de los sistemas de información compromete a todos los miembros de la organización.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. 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.

viii. 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.

ix. 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 de la seguridad

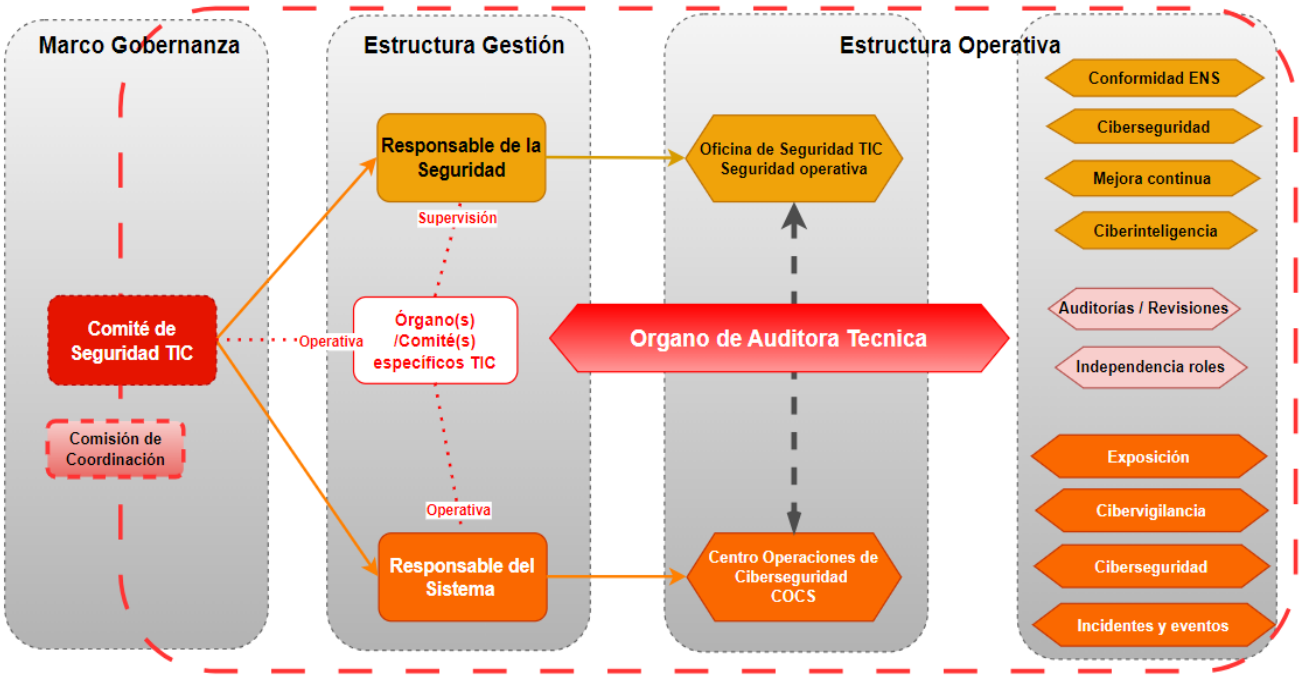
La presente PSI implica un modelo de gobernanza centralizado considerando las necesidades que presenta el servicio asistencial, por cuando se requieren una serie de servicios periféricos territorialmente desplegados.

Este modelo se desarrolla en forma piramidal, con una capa superior coronada por los órganos de gobierno y dirección estratégica, seguida del estrato de mandos intermedios operativos y finalizada sobre la base de la pirámide por la estructura táctica.

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.

La estructura puede contemplar oficinas de seguridad técnicas, servicios de seguridad, órganos y subróganos de coordinación, servicios técnicos y servicios de auditoría, área de seguimiento e inteligencia, o cualquier otro que pudiera ser requerido.

Se deberán considerar las dependencias y las interconexiones y flujos requeridos entre distintas entidades públicas y otras entidades territoriales diferenciadas.



Modelo de Gobernanza

10.3 Roles y Órganos de la Seguridad de la Información

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.

(NOTA: podrían ser los jefes de servicios o responsables de los diferentes órganos y unidades administrativas. Puede considerarse una máxima autoridad administrativa, para que asuma estas funciones.)

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.

(NOTA: podrían ser los gerentes de entidades públicas, jefes de servicios o responsables de los diferentes órganos y unidades administrativas. Puede considerarse una máxima autoridad administrativa, para que asuma estas funciones.

Para mejorar la identificación de la información y su valoración, podrán designarse subdelegados de servicios o información en los niveles inferiores, por ejemplo, Centros de Atención Primaria u Hospitalaria, en función de las características específicas de estos.)

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

Para mejorar la identificación de los servicios y su valoración, así como la información, podrán designarse subdelegados de servicios o información en los niveles inferiores, por ejemplo, en los Centros de Atención Primaria u Hospitalaria, en función de las características específicas de estos.

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 la 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.

Cuando corresponda se podrá declarar a la persona física que ostente este rol con la responsabilidad o representación de la /del [ENTIDAD/ORGANIZACIÓN/ORGANISMO], en la aplicación de las medidas para gestionar los riesgos de ciberseguridad derivados de la aplicación de la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

(NOTA: este rol debe ser designado expresamente. El Responsable de la Seguridad corresponderá a un cargo o funcionario, de nivel ejecutivo, designado formalmente por los órganos correspondientes de seguridad.

Podrá ser el Secretario General de la Consejería, responsable de servicios o entidades públicas.

El responsable de seguridad podrá apoyarse en terceros para la ejecución de tareas y funciones concretas.

Podrán crearse y/o desplegarse oficinas de seguridad, en las que podrá apoyarse el Responsable de la Seguridad.)

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.

(NOTA: Podrá ser designado como tal, el Director o Jefe de Servicio del Área de TI, Director General con competencias digitales o de tecnologías, responsables de empresas públicas de tecnología encargadas de las prestaciones tecnológicas…)

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.

10.4 Delegado de Protección de Datos

En aquellas instituciones y Administraciones a las que afecta esta PSI, que hayan procedido a la designación de un delegado de protección de datos, podrán 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.

10.5 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: Consejero/a con competencias en Sanidad o alto cargo al que este delegue de manera expresa.
- 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/departamentos del sector de salud. 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:

i. 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.

j. Coordinar a los diferentes órganos y roles de seguridad de la información.

k. Resolver conflictos de responsabilidad entre diferentes órganos y/o responsables y/o áreas/ departamentos.

l. Establecer los mecanismos de cooperación y coordinación en sanidad en materia de seguridad de la información, con otros órganos [inter]territoriales [inter]ministeriales, y/o de seguridad de la información.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. 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.

10.6 Comisión de coordinación

Cuando el comité lo consideré oportuno se creará una **Comisión de Coordinación** para la adecuada coordinación de los diferentes niveles y roles designados.

Su principal función será la coordinación de las acciones de los diferentes roles y órganos designados o constituidos al amparo de esta PSI, elevando las propuestas de mejora o discrepancias al Comité de Seguridad:

- Coordinar la acción de las/ de los [AREAS/GERENCIAS/DEPARTAMENTOS] en materia de seguridad de la información y resolver, inicialmente, las posibles discrepancias.
- Asesorar en materia de Seguridad de la Información.
- Resolver, inicialmente, los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades organizativas, pudiendo elevarlas al Comité de Seguridad de la Información.
- Proponer al Comité de Seguridad acciones para la mejora continua del sistema de gestión de la Seguridad de la Información.

10.7 Oficina de Seguridad TIC

Dentro de la estructura de gobernanza de la ciberseguridad para la prestación de servicios sanitarios, se podrá constituir la **Oficina de Seguridad TIC**[1], que apoyará en sus funciones al Responsable de la Seguridad, y cuyas competencias estarán relacionadas con la adecuación al ENS, normativa y gestión de riesgos, análisis y mejora continua, seguridad en las interconexiones y conectividad, y otras funciones conexas o concordantes.

Para su **composición** se propone:

- El **Director de la Oficina**, a propuesta del Responsable de la Seguridad y nombrado por el Comité de Seguridad, que actuará como enlace con el

[1] Se puede considerar también la posibilidad de englobar en una única Oficina de Seguridad las funciones de seguridad TIC, la de las personas, la de las infraestructuras, la de la documentación, etc.

mismo, que será el **Responsable de la Seguridad (RSEG)**, o la persona en quien delegue.

- **Secretario de la Oficina**, a propuesta del Responsable de la Seguridad y nombrado por el Comité de Seguridad TIC, a propuesta de los miembros de la Oficina de Seguridad.
- Todos aquellos **administradores especialistas de seguridad (AES)** que el Responsable de la Seguridad determine que sean necesarios.

Las **funciones de la Oficina de Seguridad TIC** serán, entre otras que les puedan ser encomendadas por el Comité de Seguridad TIC:

a) Gestionar la operativa de la seguridad con la finalidad de realizar la adecuación, Implantación y gestión de la Conformidad con el ENS.
   - Analizar y gestionar los riesgos.
   - Desplegar medidas relacionadas con la operativa del sistema.
   - Desarrollar mantener la normativa de seguridad y elevar a su aprobación.

b) Redactar y presentar propuestas al Comité de Seguridad TIC, en aspectos relacionados con la ciberseguridad y los debatirá en primera instancia, para ser trasladados al Comité.
   - Proponer planes directores de ciberseguridad.
   - Planificar adecuaciones a normas relacionadas con la ciberseguridad de impacto en la prestación sanitaria.
   - Analizar y desplegar planes de adecuación de perfiles específicos de seguridad que pudieran ser de aplicación a la prestación sanitaria.
   - Desarrollar planes de continuidad y estrategias de contingencia.
   - Proponer estudios relacionados con herramientas de ciberseguridad adecuadas para el ecosistema de la prestación sanitaria.

c) Desarrollar acciones para mantener una mejora continua del sistema de gestión de la Seguridad de la Información:
   - Elaborar (y revisar regularmente) la PSI para su traslado al Comité de Seguridad TIC para su revisión, previa aprobación del órgano superior.
   - Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
   - Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de seguridad de la información y protección de datos.
   - Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

- Proponer planes de mejora de la seguridad de la información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Realizar un seguimiento de los principales riesgos residuales asumidos y recomendar posibles actuaciones respecto de ellos.
- Promover la realización de las auditorías periódicas ENS que permitan verificar el cumplimiento de las obligaciones en materia de seguridad de la Información y protección de datos.

d) Acciones de inteligencia y análisis pertinente de la información de seguridad proveniente de diferentes fuentes.

- Elaboración de informes de ciberinteligencia para la prestación sanitaria.
- Elaborar informes relacionados con los indicadores de compromiso [IOC] detectados en la prestación sanitaria.
- Desarrollo de procedimientos para mantener la proactividad en las acciones de seguridad de los servicios.
- Promover escenarios y estrategias de gestión de malware y otros eventos similares.

Periodicidad de las reuniones y adopción de acuerdos:

- El Director de la Oficina de Seguridad TIC convocará las reuniones de trabajo de sus miembros y recabará los acuerdos alcanzados, de los que dará cuenta al Comité de Seguridad TIC, para su aprobación, en su caso.
- La Oficina podrá desarrollar sus funciones en pleno o en Grupos de Trabajo para el análisis y realización de propuestas específicas. Las propuestas planteadas en la Oficina de Seguridad TIC serán sometidas a análisis, debate y aprobación, si procede, por parte del Comité de Seguridad TIC.
- Se reunirá, al menos, una vez al mes y siempre antes de las celebraciones del Comité de Seguridad TIC.

10.8 Centro de Operaciones de Ciberseguridad (COCS)

A todos los efectos se podrá constituir un **Centro de Operaciones de Ciberseguridad** (COCS) que apoyará al Responsable del Sistema y que prestará servicios de ciberseguridad, desarrollando la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TIC, a la vez que mejora la capacidad de respuesta del sistema ante cualquier ataque.

Estará bajo la dependencia del Responsable del Sistema, quien designará a quien se encargará de su dirección y realizará los pertinentes reportes periódicos al Comité de Seguridad TIC.

El Centro de Operaciones de Ciberseguridad (COCS) presta servicios de ciberseguridad, desarrollando la capacidad de vigilancia y detección de amenazas en la operación diaria de los sistemas TIC, análisis de la superficie de exposición y mejora de la capacidad de respuesta del sistema ante cualquier ataque.

El Centro de Operaciones de Ciberseguridad (COCS) llevará a cabo las siguientes funciones:

a) Analizar la superficie de exposición de los servicios de prestación sanitaria:
   - Vigilar y monitorizar la seguridad de los sistemas, y de los dispositivos de defensa
   - Vigilar y monitorizar la seguridad de los *ImT* [The Internet of Medical Things]
   - Análisis de información empleable para potenciales ataques (leaks, direcciones IP, dominios, metadatos, RRSS, …)
   - Preparar analíticas de datos relacionados con la superficie de exposición y reporte a la Oficina de Seguridad TIC.
   - Gestionar vulnerabilidades (análisis y determinación de las acciones de subsanación/parcheado) de aplicaciones y servicios.
   - Promover análisis automatizados o dirigidos de seguridad sobre la infraestructura o servicios, y específicamente análisis de vulnerabilidades y pruebas de denegación de servicios.

b) Servicio de cibervigilancia que posibilite la prospectiva sobre la ciberamenaza:
   - Recopilar avisos de vulnerabilidades y amenazas publicadas por los CSIRT, organismos y fabricantes.
   - Monitorizar suplantaciones.
   - Servicios de monitorización de fuentes abiertas para detectar con antelación posibles ataques organizados.
   - Recopilar y obtener la información necesaria para la ciberinteligencia y coordinación con las necesidades de la Oficina de Seguridad TI.

c) Servicio de ciberseguridad
   - Monitorizar y realizar seguimiento de las anomalías del sistema y de las redes.
   - Analizar y correlar eventos de seguridad y registros de actividad de los sistemas.
   - Realizar configuraciones y mantenimiento de los componentes asociados a las operaciones de seguridad y dispositivos de defensa.

d) Servicio de apoyo a incidentes:
   - Apoyar la resolución de incidentes y eventos.

- En su caso, constituir un Equipo de Respuesta a Incidentes de Seguridad: Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Mantener un Servicio de Alerta Temprana (SAT) de alertas de seguridad en las redes corporativas y en las conexiones a Internet de los sistemas.
- Realizar el análisis forense digital y de seguridad.

Cualquier Área/Servicio TI implicado con la prestación de servicios de asistencia sanitaria, deberá, por un lado, coordinarse con la Oficina de Seguridad TIC en la definición y aplicación de las medidas de seguridad en los sistemas e infraestructuras que estén bajo su responsabilidad; y por el otro, colaborar con el Centro de Operaciones de Ciberseguridad (COCS) en las tareas de operativa diaria.

En el caso que, por su tamaño o falta de recursos, no disponga de un COCS, un servicio Área/Servicio TI que pueda desarrollar servicios para la prestación sanitaria, podrá asumir, en colaboración con la Oficina de Seguridad TIC, en todo o en parte, las funciones descritas anteriormente.

10.9 Órgano de Auditoria Técnica

Dentro de la estructura organizativa del marco de gobernanza de ciberseguridad, podrá constituirse un Órgano de Auditoría Técnica (OAT) independiente, para la realización de auditorías de conformidad de los sistemas. Este órgano podrá asumir las supervisiones relativas a medidas desplegadas para gestionar los riesgos de ciberseguridad de los sistemas de redes y de información utilizados para prestar servicios.

Deberá preservar su independencia del resto de la estructura técnica y de seguridad y la ausencia de conflicto de intereses entre los elementos auditor y auditado.

Cuando sea constituido, se procederá a su correspondiente proceso de acreditación conforme a las normas establecidas por la autoridad de control.

Realizará los procesos de auditoria periódicas, según criterios y modelo establecido.

10.10 Otros Roles o Responsabilidades.

Podría considerarse otros roles de seguridad que pudieran ser necesarios por imperativo legal, y normas particulares que detalles obligaciones específicas a cualquiera de los distintos órganos y entidades del sector público implicados en los servicios sanitarios.

10.10.1 Responsable de la seguridad física.

Podrá considerarse a las personas con responsabilidad en la seguridad física de las instalaciones asignadas para la prestación de servicios sanitarios.

Velará por la protección de las instalaciones, para alinear los requerimientos de seguridad con las medidas de seguridad físicas y lógicas.

Esta función podrá ser asumida por el rol relacionado con la ciberseguridad de los sistemas de redes y de información utilizados para prestar servicios.

10.10.2 Responsable de proveedores sanitarios

Podrá considerarse a las personas con responsabilidad en los procesos de homologación, seguimiento, control y contacto con los proveedores de los servicios asistenciales con criticidad en la cadena de suministro.

Esta función podrá ser asumida por el rol relacionado con la ciberseguridad de los sistemas de redes y de información utilizados para prestar servicios.

10.10.3 Órgano de auditoría interna de seguridad

Se podrá disponer de un área o servicio independiente de la gestión de seguridad, que se encargará de las revisiones de los procesos asociados a la seguridad.

Será independiente del resto de roles descritos y solo rendirá cuentas al más alto nivel jerárquico. Se encargará de verificar los procedimientos adoptados en materia de seguridad, para asegurar que los mismos son conformes a la normativa.

En sus procesos se realizarán las comprobaciones oportunas, desplegando técnicas de muestreo y evidencias y con un programa de auditoria adecuado para la emisión de informes.

El trabajo del servicio de auditoría interna se realizará de acuerdo con normas aceptadas internacionalmente, se registrará en documentos de trabajo y se plasmará en informes y recomendaciones dirigidas a los órganos de dirección del organismo.

Para mantener el requisito de objetividad y profesionalidad necesario, este órgano podrá contar con servicios profesionales de externos, dando cumplimiento al artículo 16 del ENS.

10.11 Procedimientos de designación

El [ÓRGANO COMPETENTE] y comunicada a las partes afectadas [INDICAR COMO SE HA PROCEDIDO].

Los Responsables de las/ de los [AREA/GERENCIA/DEPARTAMENTO] serán designados por la Dirección/Gerencia.

Los roles de seguridad serán revisados cada cuatro años en el caso de que exista una vacante, la misma deberá ser cubierta en el plazo de un mes, siguiendo el mismo procedimiento.

11.Datos personales

La/El [ENTIDAD/ORGANIZACIÓN/ORGANISMO], 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.

[NOTA: en que caso de que se disponga de política de protección de datos o el servicio de salud se integre: En desarrollo de los principios de la vigente normativa de protección de datos, entre otros, los de minimización, confidencialidad o proactividad, la organización ha definido un marco de actuación en la Política de Protección de Datos, aprobada _____-]

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 la/del [ENTIDAD/ORGANIZACIÓN/ORGANISMO], 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 la/del [ENTIDAD/ORGANIZACIÓN/ORGANISMO], 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.

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. Integración en la política de la comunidad autónoma

La presente PSI se coordinará con la Política de Seguridad de la Comunidad Autónoma debiendo modificarse cuando sea modificada la de la autonomía.

Para la resolución de discrepancias se creará un Grupo de Trabajo específico en la Consejería con competencias en sanidad de la Comunidad Autónoma.

19. 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.

20. Modificaciones / control de cambios

Versión	Fecha	Modificaciones respecto a la versión anterior
01	__ de _____ de ____	

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL