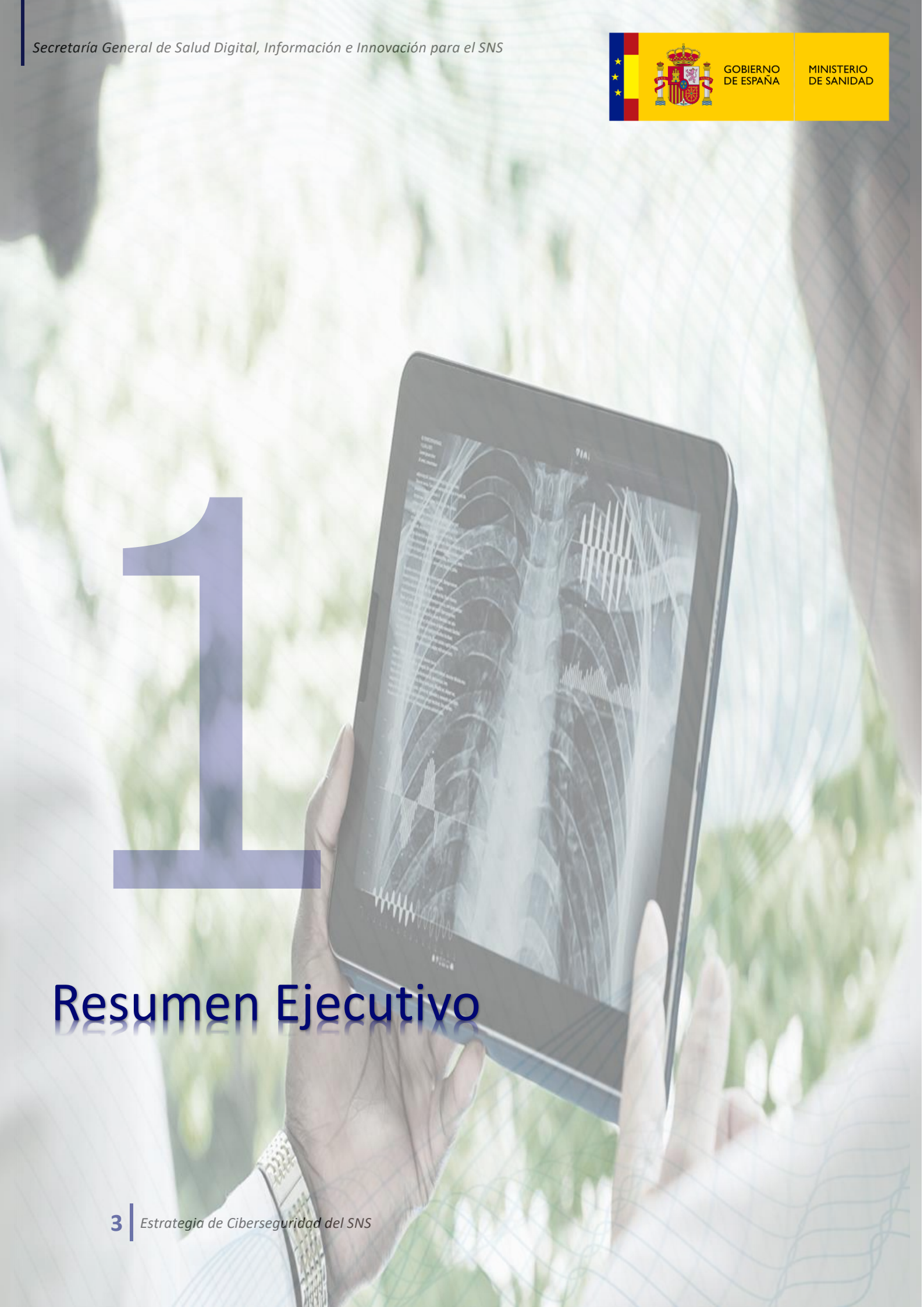
ESTRATEGIA DE CIBERSEGURIDAD

SISTEMA NACIONAL DE SALUD 2025-2028

Secretaría General de Salud Digital,
Información e Innovación para el SNS
15 de julio de 2025

GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD

Índice de Contenidos



1

Resumen Ejecutivo

La Estrategia de Ciberseguridad del SNS establece un marco integral para proteger la información sanitaria, garantizar la continuidad asistencial y fortalecer la confianza de los ciudadanos en un entorno digital seguro y resiliente.

1. Resumen ejecutivo

La Estrategia de Ciberseguridad del Sistema Nacional de Salud (SNS) se presenta como un marco integral diseñado para proteger la infraestructura de información sanitaria, garantizar la continuidad asistencial y salvaguardar la confianza de los ciudadanos en el sistema de salud. En un contexto de creciente digitalización y amenazas cibernéticas, esta estrategia se fundamenta en una misión clara: asegurar la integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad de los datos sanitarios.

La visión de esta estrategia es establecer un entorno seguro y resiliente que permita la continuidad de la atención sanitaria. Además, se aspira a posicionar al SNS como un referente en ciberseguridad, promoviendo la colaboración entre todos los actores del sistema.

La estrategia se basa en ocho objetivos estratégicos que guiarán su implementación.

01 Establecer una red de colaboración en ciberseguridad entre las Comunidades Autónomas en el Sistema Nacional de Salud.

02 Definir medidas para asegurar la integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad de los datos sanitarios.

03 Posicionar al SNS como un referente en ciberseguridad a nivel nacional y europeo.

04 Fomentar el cumplimiento normativo en ciberseguridad.

05 Establecer indicadores para gestionar el nivel de madurez en ciberseguridad.

06 Impulsar la investigación y análisis de riesgos en dispositivos médicos y tecnologías emergentes.

07 Garantizar la continuidad asistencial reforzando la resiliencia operativa y la cadena de suministro.

08 Promover la capacitación continua en ciberseguridad.

Con el propósito de alcanzar y cumplir los objetivos definidos en la Estrategia de Ciberseguridad del Sistema Nacional de Salud (SNS), se han establecido 12 ejes estratégicos los cuales deberán contextualizarse a las diferentes líneas asistenciales y modelos de gestión autonómicos. Estos ejes abarcan áreas clave que son fundamentales para garantizar la protección de la infraestructura de información sanitaria, la continuidad asistencial y la confianza de los ciudadanos en el sistema de salud. Cada eje estratégico ha sido cuidadosamente diseñado para abordar los desafíos específicos de la ciberseguridad en el ámbito sanitario, promoviendo la colaboración entre todos los actores del sistema y posicionando al SNS como un referente en ciberseguridad:

01 Gobernanza de la Ciberseguridad Sanitaria

02 Intercambio de Información de Ciberseguridad

03 Cumplimiento Regulatorio en Ciberseguridad

04 Observatorio de madurez Ciber

05 Seguridad de la información del SNS

06 Modelo de Gestión de Crisis

07 Gestión de la Cadena de Suministro

08 Mejora de la capacitación en ciberseguridad

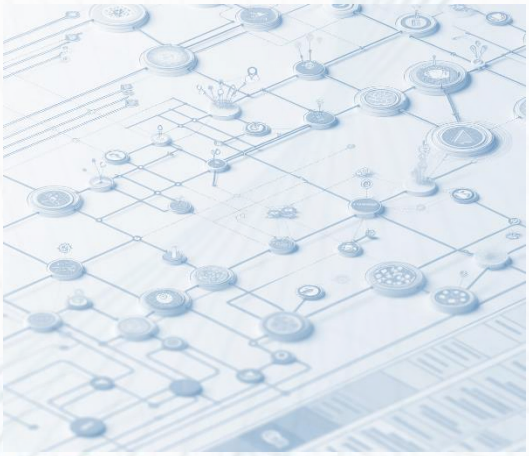
09 Liderazgo de pensamiento en Ciberseguridad

10 Optimizar el proceso de contratación de productos y servicios de ciberseguridad

11 Búsqueda de líneas financiación

12 Apoyo para la implantación de la Estrategia en los Servicios Públicos de Salud

La implementación de esta estrategia no solo busca cumplir con las normativas y directrices nacionales y europeas, sino también establecer un modelo de ciberseguridad que sirva como referencia para otros sectores. A través de un enfoque proactivo y colaborativo, se fomentará una cultura de ciberseguridad que involucre a todos los actores del sistema sanitario, asegurando así la protección de la información y la confianza de la ciudadanía en el SNS.



Por tanto, el presente documento desarrolla de manera completa la Estrategia de Ciberseguridad del Sistema Nacional de Salud, con el propósito de reforzar la protección de los Servicios Públicos de Salud.

GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD

2 Introducción

La Estrategia de Salud Digital del SNS tiene como objetivo transformar la salud pública en España mediante tecnologías digitales, empoderando a los ciudadanos y garantizando la seguridad y gestión eficiente de los datos sanitarios.

2. Introducción

La Estrategia de Salud Digital (ESD) del Sistema Nacional de Salud (SNS) tiene como objetivo mejorar y preservar la salud de la población en España, así como reforzar el sistema de salud público. Esto se logrará a través del poder transformador de las tecnologías digitales, las cuales estarán enfocadas en beneficiar a los ciudadanos, los profesionales sanitarios, las entidades que ofrecen Servicios Públicos de Salud y otros actores implicados.

Como punto de partida relevante sobre el que sentar las bases de la presente Estrategia de Ciberseguridad del Sistema Nacional de Salud, se debe de considerar la Estrategia Nacional de Ciberseguridad del 2019 que establece la posición de España ante una nueva concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional y establece un objetivo claro: garantizar a los ciudadanos un uso seguro y fiable del ciberespacio, protegiendo los derechos y libertades de los ciudadanos.

Teniendo en cuenta la creciente digitalización en los Servicios Públicos de Salud de las Comunidades Autónomas, los cuales han ido incorporando nuevos servicios y funcionalidades a los ciudadanos mediante el uso de la Inteligencia Artificial (IA) en servicios de medicina personalizada para los pacientes gestionando datos de su historial médico o en la optimización de los recursos dentro del sistema así como recientemente la implantación del Espacio Europeo de Datos Sanitarios (EEDS), que capacitará a las personas para que asuman el control de sus datos sanitarios y facilitará el intercambio de datos para la prestación de asistencia sanitaria en toda la Unión Europea, supone un nuevo paradigma en la gestión y seguridad de los datos para el Ministerio de Sanidad (MSAN) y los Servicios Públicos de Salud de las CCAA. La Directiva Europea sobre Seguridad de las Redes y los Sistemas Informáticos (SRI2 o NIS2), que tiene por objetivo crear un nivel común de ciberseguridad en todos los Estados miembros de la Unión Europea, define al Sector Salud como de alta criticidad, lo que impone una serie de obligaciones en materia de ciberseguridad que deben ser contempladas.

La ciberseguridad debe dar confianza al ciudadano frente a los riesgos derivados de la generalización del uso de la tecnología y la elevada conectividad entre dispositivos/sistemas que tratan su información sanitaria.

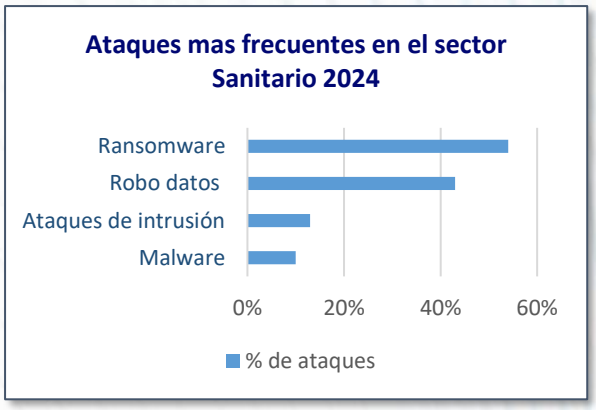
GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD

3 Contexto

3. Contexto

En la actualidad, la ciberseguridad se ha convertido en un aspecto crítico para el Sistema Nacional de Salud (SNS) en España, donde la digitalización ha transformado el modelo asistencial y los procesos administrativos. La implementación de tecnologías avanzadas, como la Historia Clínica Digital y la telemedicina, así como la incorporación constante de tecnología en los servicios de salud (IoT, IoMT, etc.) ha mejorado la eficiencia y el acceso a la información, pero también ha incrementado la vulnerabilidad y exposición ante ciberataques. Los cibercriminales han intensificado sus esfuerzos, buscando información médica para llevar a cabo fraudes y extorsiones, lo que ha resultado en un aumento significativo de incidentes de seguridad, incluidos ataques de ransomware y phishing.

> *Los Servicios Públicos de Salud se enfrentan a crecientes ciberamenazas que ponen en riesgo la confidencialidad de los datos y la continuidad asistencial. La presente estrategia pretende dotar de herramientas y capacidades para evolucionar y protegerse.*



Datos de 2024 según INCIBE

https://www.incibe.es/incibe-cert/blog/ciberseguridad-en-el-sector-salud-caracteristicas-amenazas-y-recomendaciones

Estos ataques no solo amenazan la privacidad de los pacientes, sino que también pueden interrumpir la operatividad de los Servicios Públicos de Salud, generando consecuencias devastadoras que van desde la pérdida de confianza pública hasta sanciones legales. En este contexto, la Directiva Europea sobre Seguridad de las Redes y los Sistemas Informáticos (NIS2) clasifica al sector salud como de alta criticidad, lo que impone una serie de obligaciones en materia de ciberseguridad. Esta normativa busca establecer un nivel común de protección en todos los Estados miembros de la Unión Europea, lo que subraya la necesidad de que el SNS adopte medidas robustas para cumplir con estos requisitos.

La creciente presión regulatoria y la falta de uniformidad en las medidas de ciberseguridad entre las diferentes Comunidades Autónomas añaden un nivel adicional de riesgo. Un punto débil en una parte del sistema puede comprometer la integridad de otros, lo que pone de manifiesto la importancia de establecer un enfoque coordinado y colaborativo en la gestión de la ciberseguridad. La interconexión entre servicios, aunque facilita el acceso a la atención, también expone al SNS a posibles vulnerabilidades.

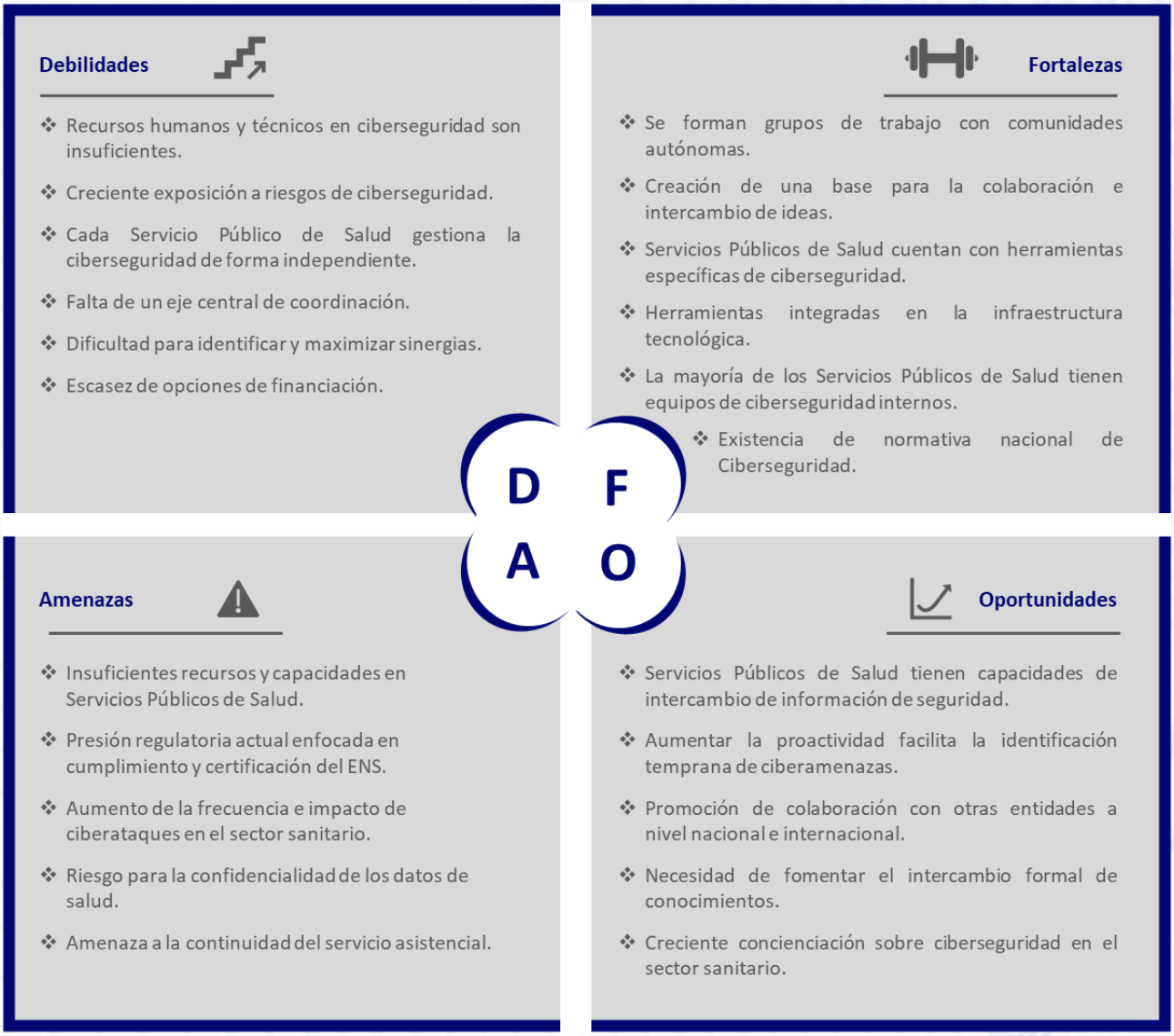
Ante este panorama, se hace imprescindible desarrollar una estrategia de ciberseguridad unificada que aborde las debilidades existentes y anticipe futuras amenazas. Esta estrategia no solo debe centrarse en la protección de los datos, sino también en la formación y capacitación continua del personal, asegurando que todos los actores del SNS estén preparados para identificar y responder a ciberamenazas. La colaboración entre entidades públicas y privadas es esencial para construir un enfoque efectivo y compartido, lo que permitirá mejorar la resiliencia del sector ante los desafíos cibernéticos.

Adicionalmente, la creación del Espacio Europeo de Datos Sanitarios (EEDS) representa un nuevo paradigma en la gestión y seguridad de los datos para el Ministerio de Sanidad y los Servicios Públicos de Salud de las Comunidades Autónomas. Este espacio capacitará a los ciudadanos para que asuman el control de sus datos sanitarios y facilitará el intercambio de información para la prestación de asistencia sanitaria en toda la Unión Europea.

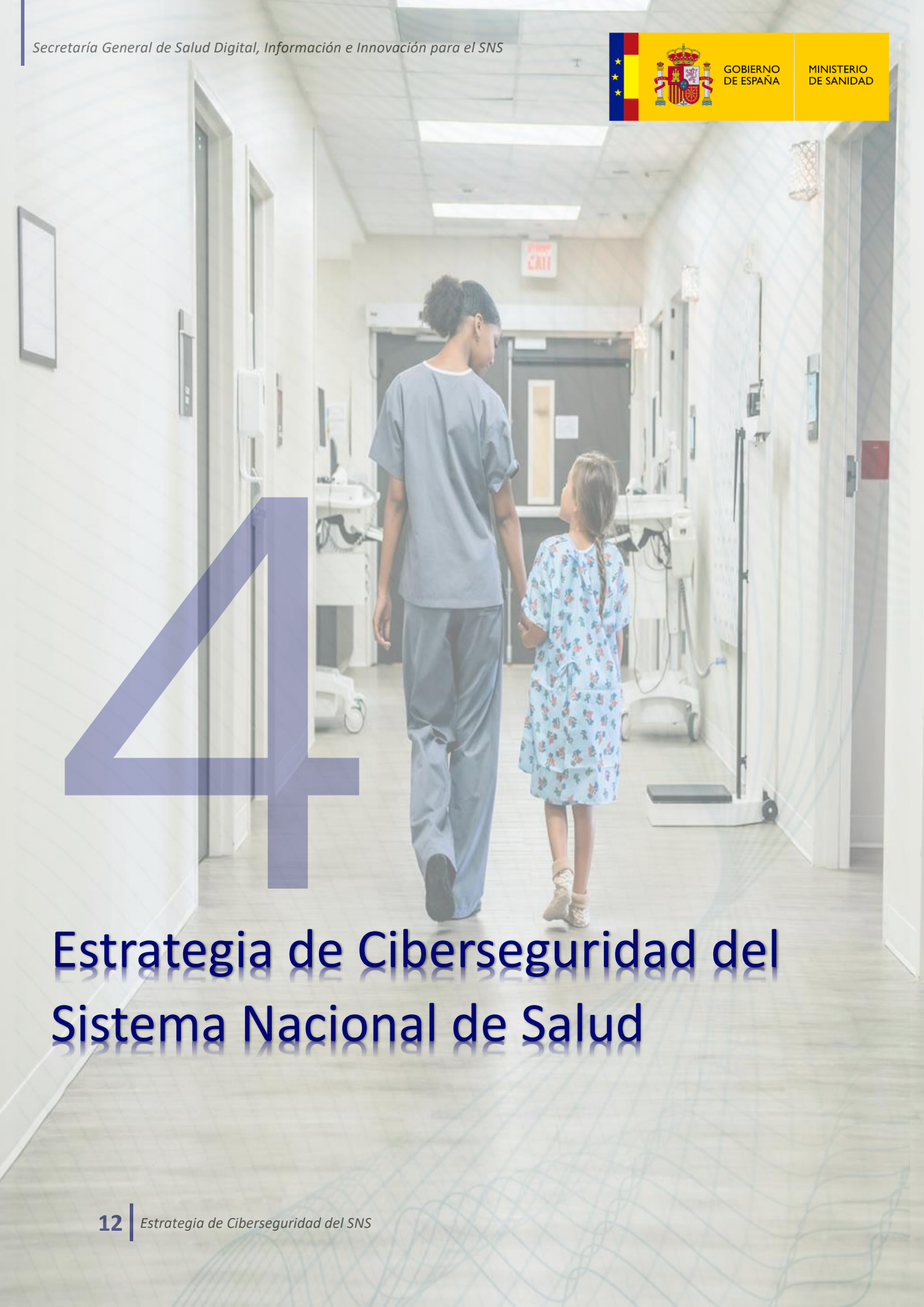
Dentro de este contexto, es importante destacar los cambios y desafíos que ha traído consigo la implementación de la Inteligencia Artificial (IA) en los Servicios Públicos de Salud. Se han introducido sistemas de IA en servicios de diagnóstico y tratamiento, en medicina personalizada para los pacientes, considerando datos de su historial médico, y en la optimización de los recursos del sistema sanitario. Estas innovaciones presentan una serie de retos en cuanto a ciberseguridad, como garantizar la privacidad y seguridad de los datos sanitarios, la aplicación de nuevas normativas y regulaciones, los aspectos técnicos de la integración de sistemas, y la capacitación y formación de los profesionales en el uso de estas herramientas.

En resumen, el contexto actual de ciberseguridad en el sector salud es complejo y desafiante. La digitalización ha traído consigo tanto oportunidades como riesgos, y es fundamental que el SNS adopte un enfoque proactivo y coordinado para proteger la información sanitaria y garantizar la continuidad de los Servicios Públicos de Salud. La Estrategia de Ciberseguridad del SNS se presenta como una respuesta integral a estos desafíos, estableciendo un marco que no solo busca cumplir con las normativas vigentes, sino también posicionar al SNS como un referente en ciberseguridad a nivel nacional y europeo.

La situación actual en materia de ciberseguridad del SNS cuenta con una serie de características particulares, pudiendo esquematizarse a través de un análisis interno (Debilidades y Fortalezas) y de uno externo (Amenazas y Oportunidades):



GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD



4

Estrategia de Ciberseguridad del Sistema Nacional de Salud

4. Estrategia de Ciberseguridad del Sistema Nacional de Salud

La Estrategia de Ciberseguridad del Sistema Nacional de Salud se desarrolla en un contexto de creciente digitalización y transformación tecnológica en el sector sanitario, donde la adopción de nuevas tecnologías ha revolucionado la forma en que se gestionan y se prestan los Servicios Públicos de Salud. Esta evolución ha permitido mejorar la eficiencia, el acceso a la información y la calidad de la atención médica, pero también ha expuesto al sistema a un aumento significativo de riesgos y amenazas cibernéticas.

Esta estrategia no solo busca mitigar los riesgos asociados a los ciberataques, sino que también se fundamenta en la necesidad de establecer un marco robusto que asegure la integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad, de los datos sanitarios.

Para lograr estos objetivos, la estrategia se apoya en cinco pilares fundamentales que guiarán su desarrollo y ejecución. Estos pilares son esenciales para construir un enfoque integral y coordinado que permita al SNS enfrentar los desafíos de ciberseguridad de manera efectiva, asegurando así la protección de la información y la confianza de la ciudadanía en el sistema de salud.

Un marco robusto y cinco pilares fundamentales protegen la integridad y confianza en el sistema de salud digital.

4.1 Alcance, misión y visión

Con un enfoque integral y coordinado, la estrategia de ciberseguridad del SNS define su alcance, misión y visión para proteger la información sanitaria y garantizar la confianza en el sistema de salud. Solo de esta manera se pueden definir las bases sobre las cuales se diseña la misma.

Alcance

El alcance de la Estrategia de Ciberseguridad del SNS abarca:

Ministerio de Sanidad	Servicios Públicos de Salud
Definir al Ministerio de Sanidad como el ente rector que guiará y supervisará la implementación de la estrategia en todo el sistema.	Incluir todos los Servicios Públicos de Salud de las Comunidades Autónomas y del Instituto Nacional de Gestión Sanitaria (INGESA), asegurando que las medidas de ciberseguridad se apliquen de manera homogénea y efectiva en todas las entidades que conforman el SNS.

Misión

La misión de la Estrategia de Ciberseguridad del SNS pretende, mediante un enfoque integral, fomentar la confianza de los ciudadanos en los Servicios Públicos de Salud a través de las siguientes razones concretas:

	*Proteger y asegurar la infraestructura mediante la implementación de medidas de ciberseguridad*		*Garantizar la continuidad asistencial*
	*Proteger los datos sanitarios, asegurando la interoperabilidad de los sistemas de información*		*Homogeneizar el nivel de madurez en ciberseguridad de los diferentes actores del SNS*

Visión

A su vez, la visión sobre la Estrategia de Ciberseguridad del SNS establece hacia dónde queremos ir, representando así la aspiración futura del SNS.

	***Entorno colaborativo y seguro** que permita la continuidad de la atención sanitaria, incluso ante la creciente amenaza de ataques cibernéticos.*		***Posicionar al SNS como un referente en ciberseguridad**, promoviendo la colaboración entre todos los actores del sistema y garantizando la protección de la información sanitaria.*

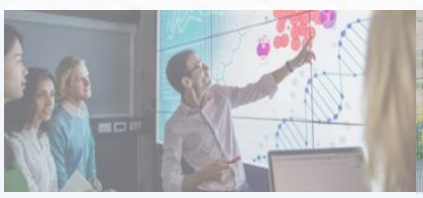
4.2 Objetivos Estratégicos

La Estrategia de Ciberseguridad del SNS se fundamenta en los siguientes objetivos estratégicos:

OB 01 **Establecer una red de colaboración en ciberseguridad** entre las 17+2 Comunidades Autónomas para el intercambio temprano sobre incidentes de ciberseguridad, con el fin de mejorar la detección, respuesta y resiliencia ante ciberataques	*Al compartir información sobre incidentes de ciberseguridad de manera temprana, se mejora la detección, respuesta y resiliencia ante ciberataques en todo el SNS.*
OB 02 **Definir medidas para asegurar** la integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad del dato sanitario.	*Implementar protocolos y prácticas que garanticen que los datos sanitarios sean íntegros, confidenciales y accesibles, asegurando su trazabilidad y autenticidad en todo momento.*
OB 03 **Posicionar al SNS como un referente** de ciberseguridad para los Servicios Públicos de Salud españoles y europeos.	*Establecer al SNS como un modelo a seguir en ciberseguridad, tanto a nivel nacional como europeo, promoviendo las mejores prácticas.*
OB 04 **Fomentar el cumplimiento normativo** en materia de ciberseguridad entre los distintos actores que conforman el SNS.	*Asegurar que todos los actores del SNS cumplan con las normativas de ciberseguridad vigentes, promoviendo un entorno seguro.*
OB 05 **Establecer indicadores** que permitan gestionar y aumentar el nivel de madurez relativo a la ciberseguridad de los Servicios Públicos de Salud.	*Desarrollar métricas que permitan evaluar y gestionar el nivel de madurez en ciberseguridad, facilitando la identificación de áreas de mejora y el progreso en la implementación de medidas de seguridad.*
OB 06 **Impulsar la investigación y el análisis de riesgos** de ciberseguridad en dispositivos médicos y tecnologías emergentes.	*Fomentar el estudio y análisis de riesgos asociados a la ciberseguridad, con el fin de anticipar y mitigar posibles amenazas en estos ámbitos.*
OB 07 **Garantizar la continuidad asistencial** reforzando la resiliencia operativa y la cadena de suministro.	*Reforzar la continuidad asistencial incluyendo proveedores y demás actores de la cadena de suministro del ecosistema del Servicio Público de Salud así como adoptar medidas de refuerzo sobre la resiliencia operativa de los Servicios Públicos de Salud.*
OB 08 **Promover la capacitación continua** en ciberseguridad, asegurando que todos los actores del SNS estén preparados para identificar y responder a ciber amenazas.	*Garantizar que todos los usuarios y profesionales del SNS reciban formación constante en ciberseguridad, preparándolos para identificar y responder de manera efectiva.*

4.3 Funciones

Para cumplir con el objetivo de proteger la información y los sistemas de salud frente a las ciberamenazas, el SNS debe asumir diversas funciones que aseguren una respuesta coordinada y efectiva en materia de ciberseguridad. A continuación, se detallan las funciones clave que deberá asumir el SNS:



Liderazgo y gobernanza

El SNS debe establecer un marco de liderazgo y gobernanza en ciberseguridad que esté alineado con el marco normativo vigente. Esto implica:

- **Definición de roles y responsabilidades:** Clarificar las funciones de cada actor dentro del SNS en relación con la ciberseguridad, asegurando que todos comprendan su papel en la protección de la información y los sistemas.
- **Coordinación interinstitucional**: Facilitar la colaboración entre el Ministerio de Sanidad, las Comunidades Autónomas y otros organismos relevantes, promoviendo un enfoque unificado en la gestión de la ciberseguridad.
- **Supervisión y evaluación**: Implementar mecanismos de supervisión para evaluar la efectividad de las políticas y procedimientos de ciberseguridad, permitiendo ajustes y mejoras continuas.

Planificación y coordinación

La planificación y coordinación son esenciales para la implantación efectiva de la Estrategia. Esto incluye:

- **Desarrollo de un plan de acción**: Crear un plan de acción que contemple objetivos claros, metas alcanzables y un cronograma de implementación, asegurando que se aborden todas las iniciativas definidas.
- **Uniformidad en la aplicación de medidas:** Garantizar que las medidas de ciberseguridad se apliquen de manera uniforme en todos los niveles del SNS, desde los hospitales hasta los centros de atención primaria, para minimizar las vulnerabilidades.
- **Integración de tecnologías:** Promover la adopción de tecnologías de ciberseguridad que sean compatibles y complementarias entre sí, facilitando una defensa en profundidad que proteja los sistemas de salud.

Capacitación y concienciación

La formación y concienciación son fundamentales para crear una cultura de ciberseguridad adecuada dentro del SNS. Esto implica:

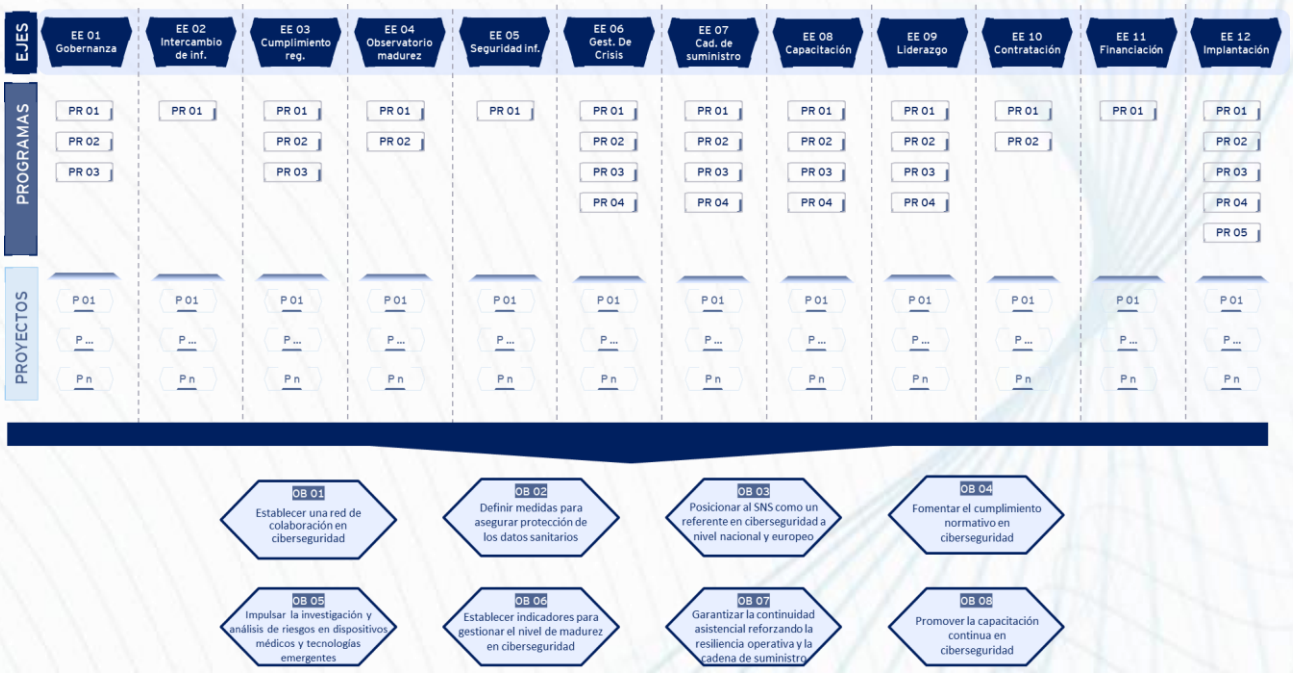
- **Programas de Formación Continua:** Implementar programas de capacitación regular que aborden las últimas tendencias en ciberseguridad, asegurando que el personal y usuarios estén al tanto de las mejores prácticas y técnicas para mitigar riesgos.
- **Simulacros de respuesta a incidentes:** Realizar ejercicios y simulacros que permitan al personal practicar la identificación y respuesta a ciberamenazas, fortaleciendo su capacidad para actuar de manera efectiva en situaciones reales.
- **Campañas de concienciación:** Desarrollar campañas de concienciación que informen a todos los actores del SNS sobre la importancia de la ciberseguridad y las medidas que pueden tomar para proteger la información y los sistemas.

4.4 Ejes estratégicos

La definición de la Estrategia de Ciberseguridad para el Sistema Nacional de Salud Español ha sido diseñada de manera estructurada disponiendo de varios elementos que permitan componer la misma y alcanzar los objetivos principales establecidos.

Según la definición de la estrategia, disponemos de los siguientes componentes:

- **Eje Estratégico:** se trata de una línea de acción que agrupa un conjunto de iniciativas y programas alineados con los objetivos estratégicos que pretende la estrategia de ciberseguridad del SNS. Estos ejes estratégicos, sirven como pilares fundamentales que guían la implementación de la estrategia de ciberseguridad, asegurando que todas las acciones estén orientadas hacia el logro y consecución de los objetivos.
- **Programa:** un conjunto de proyectos y actividades relacionadas que se gestionan de manera coordinada para alcanzar un objetivo específico dentro de un Eje Estratégico. Los programas permiten la asignación eficiente de recursos y la gestión de riesgos, facilitando la implementación de iniciativas que contribuyen a la mejora de la ciberseguridad en la organización.
- **Proyectos/Consideraciones:** es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único. En el contexto de la estrategia de ciberseguridad del SNS, un proyecto puede incluir el desarrollo de documentación, la implementación de nuevas tecnologías, la realización de auditorías de seguridad, la capacitación del personal, entre otros. Cada proyecto tiene un inicio y un final definidos, así como objetivos específicos que deben cumplirse para que el proyecto sea considerado exitoso.



La Estrategia de Ciberseguridad para el Sistema Nacional de Salud Español, se compone de **12 ejes estratégicos** los cuales son el núcleo de nuestra defensa digital. Cada uno de estos ejes está estratégicamente diseñado para abordar áreas críticas de ciberseguridad, trabajando en conjunto para crear un escudo integral que protege la información sanitaria y asegura la continuidad de los servicios públicos de salud. Este enfoque cohesivo permite al SNS enfrentar de manera efectiva los desafíos actuales y futuros en el ámbito de la ciberseguridad.

Adicionalmente, cada uno de estos ejes estratégicos está compuesto por **programas y proyectos/consideraciones** específicas que garantizan la implementación eficiente y efectiva de la estrategia de ciberseguridad del SNS. Estas iniciativas están cuidadosamente diseñadas para abordar las necesidades particulares del sistema de salud, fortaleciendo así la protección de la información sanitaria y asegurando la continuidad de los servicios públicos de salud.

4.4.1 Gobernanza de la Ciberseguridad Sanitaria

EE01

Contexto

El establecimiento de un modelo de gobierno sólido es fundamental para garantizar que todos los Servicios Públicos de Salud estén alineados en sus esfuerzos de ciberseguridad. La diversidad en la estructura organizativa y las competencias de cada Servicio Público de Salud requiere un marco claro que defina roles y responsabilidades, la capacitación necesaria para abordar las ciberamenazas de manera efectiva, así como facilitar la coordinación y el intercambio de mejores prácticas entre los diferentes actores del sistema.

Objetivos

- Definir un Modelo de Gobierno de la Ciberseguridad que contemple las particularidades de cada Servicio Público de Salud.
- Establecer roles y responsabilidades claras alineadas con las normativas vigentes.
- Crear un espacio formal de colaboración.

PR 1.1

Definición de un Modelo de Gobierno de la Ciberseguridad que sirva de base para los Servicios Públicos de Salud, contemplando los siguientes aspectos:

- Casuísticas especiales del área de ciberseguridad (pertenece a una Agencia, al propio Servicio Público de Salud, no está dedicado al Servicio Público de Salud, etc.).
- Roles y responsabilidades alineadas con los distintos requerimientos normativos (por ejemplo ENS: Guía CCN-STIC-801) y con el Marco Europeo de Competencias en Ciberseguridad elaborado por ENISA..
- Definición de una estructura organizativa tipo y dedicaciones mínimas de cada rol.
- Definición de los requerimientos mínimos de capacitación para cada rol.
- Trasladar formalmente la necesidad de contar con una estructura robusta de ciberseguridad dotada con perfiles específicos de ciberseguridad.

Creación de la Subcomisión de Ciberseguridad del SNS (dependiente de la Comisión de Salud Digital) como punto de encuentro formal para los responsables de ciberseguridad de los distintos Servicios Públicos de Salud.

PR 1.2

- Elaboración de propuestas para elevar a la Comisión de Salud Digital sobre la visión global de la ciberseguridad en el SNS.
- Fomento de la cultura de ciberseguridad del SNS.

4.4.2 Intercambio de Información de Ciberseguridad

Contexto

La coordinación efectiva entre los diferentes Servicios Públicos de Salud es esencial para enfrentar las ciberamenazas de manera conjunta. La creación de un modelo para la compartición de información sobre incidentes de ciberseguridad permitirá una respuesta más rápida y eficiente ante posibles ataques.

Objetivos

- Definir un modelo de compartición de información sobre incidentes de ciberseguridad específicos para el sector sanitario.
- Valorar la creación de un ISAC de Salud para mejorar la comunicación entre los Servicios Públicos de Salud.
- Establecer el rol de coordinación del Ministerio de Sanidad en la gestión de incidentes.

Definición y despliegue de un modelo para la compartición de información (alerta temprana) sobre incidentes de ciberseguridad, contemplando los siguientes aspectos:

- Creación de un ISAC (Information Sharing and Analysis Center) de Salud en el marco de la Red Nacional de SOC.
- Analizar alternativas con el Centro Criptológico Nacional (CCN) para la compartición de información de los Servicios Públicos de Salud (por ejemplo, creación de canales en “Element”, creación de etiquetas en “Reyes”, etc.).
- Analizar alternativas con el INCIBE para la compartición de información de las empresas proveedoras de TI para los Servicios Públicos de Salud
- Establecer las funciones de coordinación a asumir por el Ministerio de Sanidad.

4.4.3 Cumplimiento Regulatorio en Ciberseguridad

EE 03

Contexto

El cumplimiento de las regulaciones en materia de ciberseguridad es fundamental para proteger la información sanitaria y garantizar la confianza de los pacientes. Los Servicios Públicos de Salud deben disponer de una hoja de ruta clara para asegurar el cumplimiento de todas las normativas en vigor en el corto plazo, estableciendo prioridades.

Objetivos

- Definir un mapeo de controles de ciberseguridad que cubra todas las regulaciones en vigor.
- Establecer una línea base de cumplimiento y una hoja de ruta para su despliegue.
- Promover la certificación en el ENS como un objetivo estratégico para los Servicios Públicos de Salud.

PR 3.1

Generación de material de apoyo para el cumplimiento normativo:

- Definición de un modelo unificado de controles de ciberseguridad que cubra todas las regulaciones en vigor (ENS, LPIC, NIS2, LOPDPGDD).
- Definición de guías y buenas prácticas (que complementen a las emitidas por entidades oficiales) para el cumplimiento normativo en los distintos entornos (por ejemplo, entorno centralizado para atención primaria vs entorno distribuido para atención hospitalaria).
- Definición de guías y buenas prácticas adecuadas a casuísticas habituales en el sector sanitario: gestión de sistemas legacy, entornos cloud y/o externalizados, segmentación de red, interacción con entidades terceras, entre otros.
- Creación de una biblioteca de directrices y procedimientos para dar cumplimento a los distintos controles.
- Definir una línea base de cumplimiento y una posible hoja de ruta para su despliegue en los Servicios Públicos de Salud en base a las distintas tipologías (centralizados, descentralizados, agencias...), esfuerzo necesario y beneficios esperados.
- Creación de una guía de ciberseguridad en nuevas iniciativas y/o proyectos (Cybersecurity by design and by default).

Promover la certificación en el ENS como un objetivo estratégico para los Servicios Públicos de Salud.

PR 3.2

- Creación (y mantenimiento) de un mapa de Servicios Públicos de Salud certificados, con su correspondiente alcance.
- Definición de una guía para la incorporación de nuevos proyectos tecnológicos en entornos certificados.

PR 3.3

Definir guías, buenas prácticas y/o procedimientos de ciberseguridad específicos para la protección de los dispositivos médicos.

- Definición de una metodología para la Identificación y análisis de los principales riesgos y casuísticas asociadas a las distintas tipologías de dispositivo.
- Definición de mecanismos para la actualización y mejora continua del material generado.

Analizar la viabilidad de definir un Organismo de Auditoría Técnico (OAT), dentro del SNS.

PR 3.4

- Identificación de alternatives (OAT MSAN, OAT Servicio de Salud, etc.), revisión del marco competencial vigente y realización de un análisis de viabilidad técnico y presupuestario.

4.4.4 Observatorio de madurez Ciber

EE 04

Contexto

La monitorización continua del nivel de madurez en ciberseguridad de los Servicios Públicos de Salud es esencial para identificar áreas de mejora y fortalecer la protección de la información. La citada monitorización debe realizarse a partir de un conjunto de indicadores homogéneos que permita medir de manera sistemática el progreso en la implementación de medidas de ciberseguridad y compararse con otros Servicios Públicos de Salud, facilitando la identificación de buenas prácticas y lecciones aprendidas.

Objetivos

- Definir un catálogo de indicadores de ciberseguridad alineado con el ENS.
- Establecer una línea base en materia de ciberseguridad para los Servicios Públicos de Salud.
- Elaborar informes periódicos sobre el nivel de madurez y su evolución.

PR 4.1

Definir un catálogo de indicadores de ciberseguridad (alineado con el modelo unificado de controles) que permita evaluar, de forma sencilla y sistemática, el nivel de madurez (organizativa y técnica) de los distintos Servicios Públicos de Salud.

- Valorar la inclusión de fuentes objetivas y fuentes subjetivas.
- Establecer criterios claros para facilitar la información asociada a cada indicador.
- Asegurar que se incluyen indicadores y métricas para:
  - Medir el porcentaje de inversión en TIC destinado a la ciberseguridad.
  - Medir el grado de despliegue o implantación de determinadas medidas.
- Valorar/ponderar la casuística/complejidad intrínseca de cada Servicio Público de Salud.
- Valorar posible alineamiento con Informe Inés e Índice SEIS, entre otros.
- Establecer una línea base de madurez.

Elaboración, de forma periódica, de informes y cuadros de mando comparativos sobre el nivel de madurez (y su evolución) de los Servicios Públicos de Salud.

- Establecer una serie de criterios o parámetros (centralizado, descentralizado, agencia…) que permita a un Servicio Público de Salud compararse con aquellos más afines.

PR 4.2

4.4.5 Seguridad de la Información del SNS

Contexto

La protección de la información sensible en el Sistema Nacional de Salud es crucial para garantizar la privacidad de los pacientes y la integridad de los datos. Para ello, los Servicios Públicos de Salud deben ser capaces de identificar y clasificar los tipos de datos que gestionan y establecer controles adecuados para su manejo y almacenamiento, asegurando que se cumplan las normativas de ciberseguridad.

Objetivos

- Definir un mapa de Servicios/Información tipo para los Servicios Públicos de Salud.
- Definir un criterio homogéneo para categorizar los Servicios/Información
- Categorizar los Servicios/Información.

Definición de un mapa de Servicios/Información común para los Servicios Públicos de Salud con su correspondiente categorización (según ENS).

- Definición de criterios homogéneos para la categorización de los distintos Servicios/Información de un Servicio Público de Salud.

4.4.6 Modelo de Gestión de Crisis

EE 06

Contexto

A medida que los sistemas de información y los dispositivos médicos se vuelven más interconectados, también aumentan las vulnerabilidades a ciberataques que pueden comprometer la confidencialidad, integridad y disponibilidad de la información sanitaria. En los últimos tiempos, se ha registrado un elevado volumen de incidentes de ciberseguridad como el ransomware, la filtración de datos y/o los ataques a infraestructuras críticas sanitarias, provocando impactos elevados, no solo para los Servicios Públicos de Salud, si no también para la seguridad y privacidad de los pacientes.

Objetivos

- Dotar a los Servicios Públicos de Salud de herramientas para construir y/o reforzar sus capacidades de respuesta a incidentes de ciberseguridad.
- Entrenar y probar las capacidades de resiliencia y continuidad operativa de los Servicios Públicos de Salud ante incidentes cibernéticos, mediante la realización de ciberejercicios periódicos.
- Fomentar una cultura organizacional que priorice la seguridad de la información es clave en este eje estratégico

PR 6.1

Definición de un modelo de gestión de incidentes de ciberseguridad específico para los Servicios Públicos de Salud.

- Tomar como base la guía CCN-STIC 817 de Gestión de Ciberincidentes.
- Definición de roles, responsabilidades, flujos de comunicación, principales acciones a desarrollar, impacto para la sociedad, prioridades, tiempos de recuperación, etc.

Definición de un modelo de gestión de incidentes de ciberseguridad que pueda afectar a todo el SNS en su globalidad (crisis sistémica).

PR 6.2

- Tomar como base la guía CCN-STIC 817 de Gestión de Ciberincidentes.
- Definición de roles, responsabilidades, flujos de comunicación, principales acciones a desarrollar, impacto para la sociedad, prioridades, tiempos de recuperación, etc.

PR 6.3

Definir un programa de ciberejercicios periódico destinado a los distintos Servicios Públicos de Salud, contemplando, como mínimo los siguientes elementos:

- Definición de un escenario de ciberincidente específico para el sector sanitario enfocado en la gestión de la crisis por parte de la Dirección y/o los equipos técnicos.
- Definición de un marco para la evaluación homogénea de los ciberejercicios.
- Realización de los ciberejercicios en los Servicios Públicos de Salud que así lo deseen.
- Emisión de un informe de resultados personalizado para cada Servicio Público de Salud.
- Emisión de un informe de conclusiones generales sobre las capacidades de respuesta a incidentes de ciberseguridad del SNS.

Valorar la creación de un grupo de acción técnico solidario entre los distintos Servicios Públicos de Salud para apoyarse mutuamente en caso de materializarse un incidente de ciberseguridad grave.

PR 6.4

- Análisis de posibles escenarios colaboración, con sus correspondientes modelos operativos y valoración de su viabilidad técnica, presupuestaria y jurídico/laboral.

4.4.7 Gestión de la Cadena de Suministro

EE 07

Contexto

La cadena de suministro en el sector sanitario es un aspecto crítico que puede ser vulnerable a ciberataques. Los Servicios Públicos de Salud deben desplegar una metodología para gestionar el riesgo de ciberseguridad en su cadena de suministro para evaluar y mitigar los riesgos asociados a sus proveedores. Establecer controles adecuados y cláusulas contractuales específicas es esencial para garantizar la seguridad de los productos y servicios adquiridos.

Objetivos

- Definir una metodología base para la gestión del riesgo de ciberseguridad en la cadena de suministro.
- Crear un inventario de proveedores y un modelo de análisis de riesgo.
- Establecer una base de datos que establezca los requisitos y criterios para productos y servicios.

PR 7.1

Definir una metodología base para la gestión del riesgo de ciberseguridad en la cadena de suministro, contemplando los siguientes aspectos:

- Modelo de inventario de proveedores.
- Modelo de análisis de riesgo de ciberseguridad en proveedores.
- Línea base de controles de ciberseguridad para el control de los proveedores (gestión de la identidad, control de acceso, seguridad en las comunicaciones, acceso remoto, servicios en la nube…).
- Mecanismo de gestión de excepciones.

Creación (y mantenimiento) de una base de datos que contenga los requisitos mínimos para la evaluación de los proveedores, según las tipologías de productos y servicios.

PR 7.2

- Identificación de las mejores prácticas existentes en materia de gestión de proveedores en el SNS.
- Identificación de tipología de productos y servicios, y propuesta de requerimientos de seguridad a solicitar.

PR 7.3

Valorar la posibilidad de crear una familia de productos sanitarios (software y hardware) dentro del Catálogo de Productos y Servicios TIC del CCN

- Fomentar la certificación de proveedores / servicios.

Creación (y mantenimiento) de una base de datos de proveedores comunes para los distintos Servicios Públicos de Salud de cara a poder obtener ciberinteligencia sobre ellos (complementa EE 02).

PR 7.4

- Documentar las personas de contacto de cada proveedor.
- Valorar la creación de un scoring de productos/proveedores en base a criterios objetivos.

4.4.8 Mejora de la capacitación en ciberseguridad

EE 08

Contexto

La capacitación en ciberseguridad es fundamental para que todos los profesionales del SNS estén preparados para identificar y responder a ciberamenazas. Es fundamental definir itinerarios formativos específicos que se adecuen a las necesidades de formación de cada uno de los perfiles profesionales del SNS.

Objetivos

- Estratificar las necesidades de formación para los distintos perfiles profesionales.
- Definir itinerarios formativos específicos para cada perfil.
- Generar material de formación y evaluar su eficacia.

PR 8.1

Estratificar las necesidades de formación y/o concienciación para los usuarios y distintos perfiles profesionales (sanitarios, no sanitarios y TIC) del SNS.

- Identificación de los distintos perfiles profesionales que conforman el SNS y definición de sus necesidades de formación.
- Definición de un mecanismo para la revisión/actualización periódica de las necesidades de formación.

Definir un itinerario formativo y/o de concienciación para cada uno de los perfiles identificados.

- Definición de las acciones a realizar para cada uno de los perfiles identificados, para satisfacer cada una de las necesidades identificadas.
- Definición de un mecanismo para la actualización periódica de los itinerarios de formación.

PR 8.2

PR 8.3

Generar (y mantener actualizado) material de formación y/o concienciación, que complemente los cursos puestos a disposición para los diferentes perfiles.

- Elaboración de material formativo para los itinerarios definidos.
- Establecimiento de un inventario de material formativo.
- Definición de un calendario de actualización de cada elemento de material formativo.
- Valorar el despliegue de una plataforma tecnológica para la realización de las acciones formativas.

Definir mecanismos que permitan evaluar la eficacia de los itinerarios de formación y/o concienciación planteados.

- Definición de indicadores de eficacia.
- Definición de mecanismos para la medición de los indicadores definidos (por ejemplo, realización de campañas de phishing/smishing, etc.).

PR 8.4

4.4.9 Liderazgo de pensamiento en Ciberseguridad

EE 09

Contexto

El liderazgo en ciberseguridad es esencial para fomentar la innovación y la adopción de buenas prácticas en el sector sanitario.

Objetivos

- Crear grupos de trabajo que generen material sobre tecnologías aplicables en el sector sanitario.
- Definir una agenda de eventos y foros públicos relevantes para la ciberseguridad.
- Fomentar la participación activa de los actores del SNS en la discusión sobre ciberseguridad.

PR 9.1

Establecer un observatorio que analice la aparición y evolución de tecnologías emergente o nuevas normativas que pudieran tener impacto en el sector sanitario.

- Definición del conjunto de fuentes de información (técnicas y normativas) y la periodicidad de su monitorización.
- Definición de un mecanismo para la actualización del catálogo de fuentes de información a monitorizar.
- Definición de canales y mecanismos de difusión para la información recogida.

Creación de grupos de trabajo / centros de excelencia que generen material de interés (guías, buenas prácticas, etc.) sobre las distintas tecnologías de aplicación en el sector sanitario (IA, RPA, 5G, telemedicina, electromedicina).

PR 9.2

- Valorar la creación de los grupos de trabajo como subgrupos de la Subcomisión de Ciberseguridad del SNS.
- Definición del mecanismo para la gestión del ciclo de vida de los grupos de trabajo.
- Definición del mecanismo para la gestión/operación de los grupos de trabajo.

PR 9.3

Creación de grupos de trabajo para anticiparse y formar una opinión sobre el impacto en materia de ciberseguridad del uso de las tecnologías emergentes y/o las nuevas normativas.

- Valorar la creación de los grupos de trabajo como subgrupos de la Subcomisión de Ciberseguridad del SNS.
- Definición del mecanismo para la gestión del ciclo de vida de los grupos de trabajo.
- Definición del mecanismo para la gestión/operación de los grupos de trabajo.

Definir (y mantener) una agenda / inventario de eventos y foros públicos relevantes para la ciberseguridad en el ámbito sanitario.

PR 9.4

- Fomentar participación activa.
- Evangelizar sobre la importancia de los foros/eventos.

4.4.10 Optimizar el proceso de contratación de productos y servicios de ciberseguridad

EE 10

Contexto

La contratación de productos y servicios de ciberseguridad debe ser un proceso ágil y eficiente para garantizar que los Servicios Públicos de Salud puedan acceder a las soluciones necesarias para protegerse contra ciberamenazas.

Objetivos

- Explorar vías de contratación que simplifiquen el proceso de adquisición de productos y servicios de ciberseguridad.
- Establecer un repositorio de pliegos tipo para la licitación de productos y servicios.

PR 10.1

Explorar vías de contratación, compatibles con la LCSP, que simplifiquen el proceso de contratación de productos y servicios por los Servicios Públicos de Salud.

- Enumeración de las posibles vías de contratación existentes detallando sus peculiaridades.

Establecer (y mantener) un repositorio de requisitos de ciberseguridad mínimos y homogéneos para la licitación de los productos y servicios más habituales.

PR 10.2

Se propone valorar requisitos como:

- Requisitos de certificación (ENS, ISO/IEC 27001, EUCC).
- Declaración de conformidad de seguridad.
- Evaluaciones independientes.
- Preferencia a fabricantes con estándares europeos de ciberseguridad.

4.4.11 Búsqueda de líneas financiación

EE 11

Contexto

La disponibilidad de financiación es crucial para implementar medidas de ciberseguridad efectivas en los Servicios Públicos de Salud. Una búsqueda activa de financiación es esencial para garantizar la sostenibilidad de las iniciativas de ciberseguridad en el sector sanitario.

Objetivos

- Establecer un observatorio para monitorizar la disponibilidad de fondos a nivel europeo y nacional.
- Identificar oportunidades de financiación para los Servicios Públicos de Salud.
- Apoyar la implementación de estrategias de ciberseguridad mediante la búsqueda activa de financiación.

PR 11.1

Establecer un observatorio que monitorice la disponibilidad de fondos tanto a nivel europeo como nacional.

- Definición del conjunto de fuentes de información y la periodicidad de su monitorización.
- Definición de canales y mecanismos de difusión para la información recogida.

4.4.12 Apoyo para la implantación de la Estrategia en los Servicios Públicos de Salud

EE 12

Contexto

La adopción efectiva de la Estrategia de Ciberseguridad en los Servicios Públicos de Salud es crucial para garantizar la protección de la información y la resiliencia ante ciberamenazas. Asimismo, es relevante que la Estrategia sea un vehículo vivo y mantenga actualizada y relevante ante las cambiantes amenazas cibernéticas.

Objetivos

- Sensibilizar a la Alta Dirección de los Servicios Públicos de Salud sobre la importancia de la implantación efectiva de la Estrategia.
- Apoyar a las Servicios Públicos de Salud en la adopción de la Estrategia.
- Establecer un mecanismo de recogida de feedback periódico de los Servicios Públicos de Salud.

PR 12.1

Presentación de la estrategia a la Alta Dirección de los Servicios Públicos de Salud de cara a trasladar la importancia de la ciberseguridad y fomentar la implantación de la Estrategia.

- Valorar presentación individualizada para cada Servicio Público de Salud.

Definición de una guía para la adopción de la Estrategia en los Servicios Públicos de Salud, indicando prioridades básicas asociadas a los riesgos del sector.

PR 12.2

- Propuesta de medidas a desplegar en función del nivel de madurez de cada Servicio Público de Salud. Estableciendo, en su caso, prerrequisitos y correquisitos.
- Elaboración y mantenimiento de un catálogo de grupos de trabajo de la Estrategia.

PR 12.3

Establecer un mecanismo para la recogida de feedback periódico de los Servicios Públicos de Salud de cara a identificar problemáticas asociadas a la implantación de la Estrategia, así como áreas de mejora y/o aspectos no cubiertos que deban ser recogidos en sucesivas actualizaciones.

- Definición de los mecanismos y periodicidad para la recogida de feedback.

Creación de una plataforma de colaboración en materia de ciberseguridad para todos los actores del SNS en el que se puedan contrastar experiencias, crear grupos de trabajo, crear solicitudes de colaboración y/o realizar solicitudes de soporte sobre la ECSNS.

PR 12.4

- Plataforma de gestión de conocimiento.
- Definir la figura del “coordinador de conocimiento” (o moderador del foro).

PR 12.5

Monitorización del grado de avance de despliegue de la Estrategia. Monitorización de los indicadores definidos.

- Definición y monitorización de indicadores de avance.
- Creación y actualización de un Cuadro de Mando de seguimiento de la Estrategia.
- Definición de mecanismos para compartir el grado de avance.

5 Cumplimiento de los objetivos estratégicos

5. Cumplimiento de los objetivos estratégicos

La Estrategia de Ciberseguridad del Sistema Nacional de Salud (SNS) se fundamenta en los ocho objetivos estratégicos (OB) anteriormente descritos que buscan fortalecer la protección de la información sanitaria y garantizar la continuidad de los Servicios Públicos de Salud. Para alcanzar estos objetivos, los ya descritos doce ejes estratégicos (EE) actúan como mecanismos operativos específicos, cada uno de ellos diseñado para abordar áreas clave de la ciberseguridad. Estos ejes estratégicos están interrelacionados y se complementan entre sí, creando un marco cohesivo que permite al SNS responder de manera integral a los desafíos de ciberseguridad.

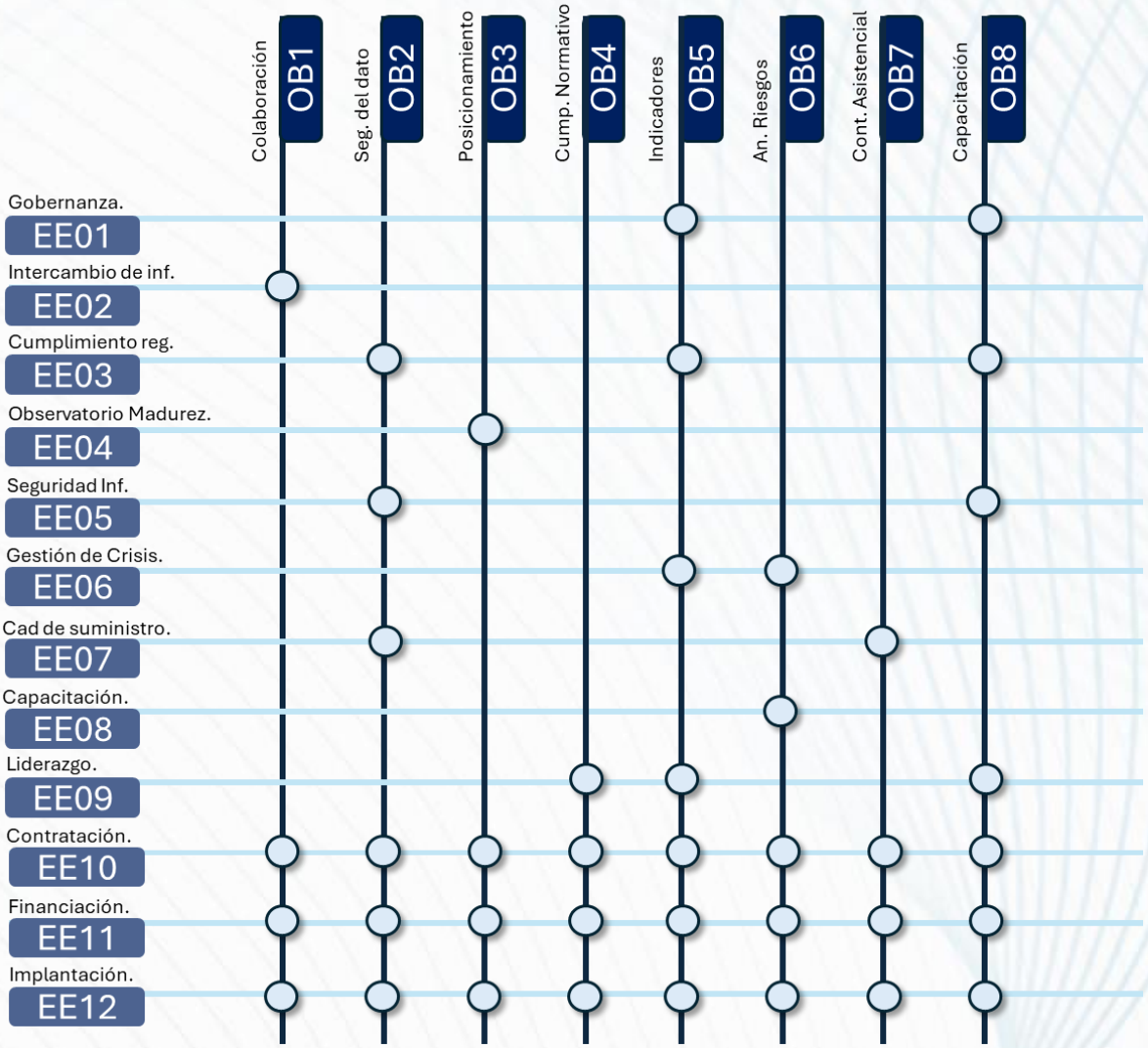
Los 12 ejes estratégicos del SNS forman un escudo integral que garantiza la protección y continuidad de nuestros Servicios Públicos de Salud.
Una buena planificación a lo largo del tiempo es esencial para su implantación.

Mapeo de cada una de las Líneas de acción definidas con los objetivos estratégicos que pretende cubrir la presente Estrategia de Ciberseguridad del SNS.

Hoja de ruta a tres años, donde se identifica el eje temporal sobre el cuál se debe de desarrollar cada una de las líneas de acción.

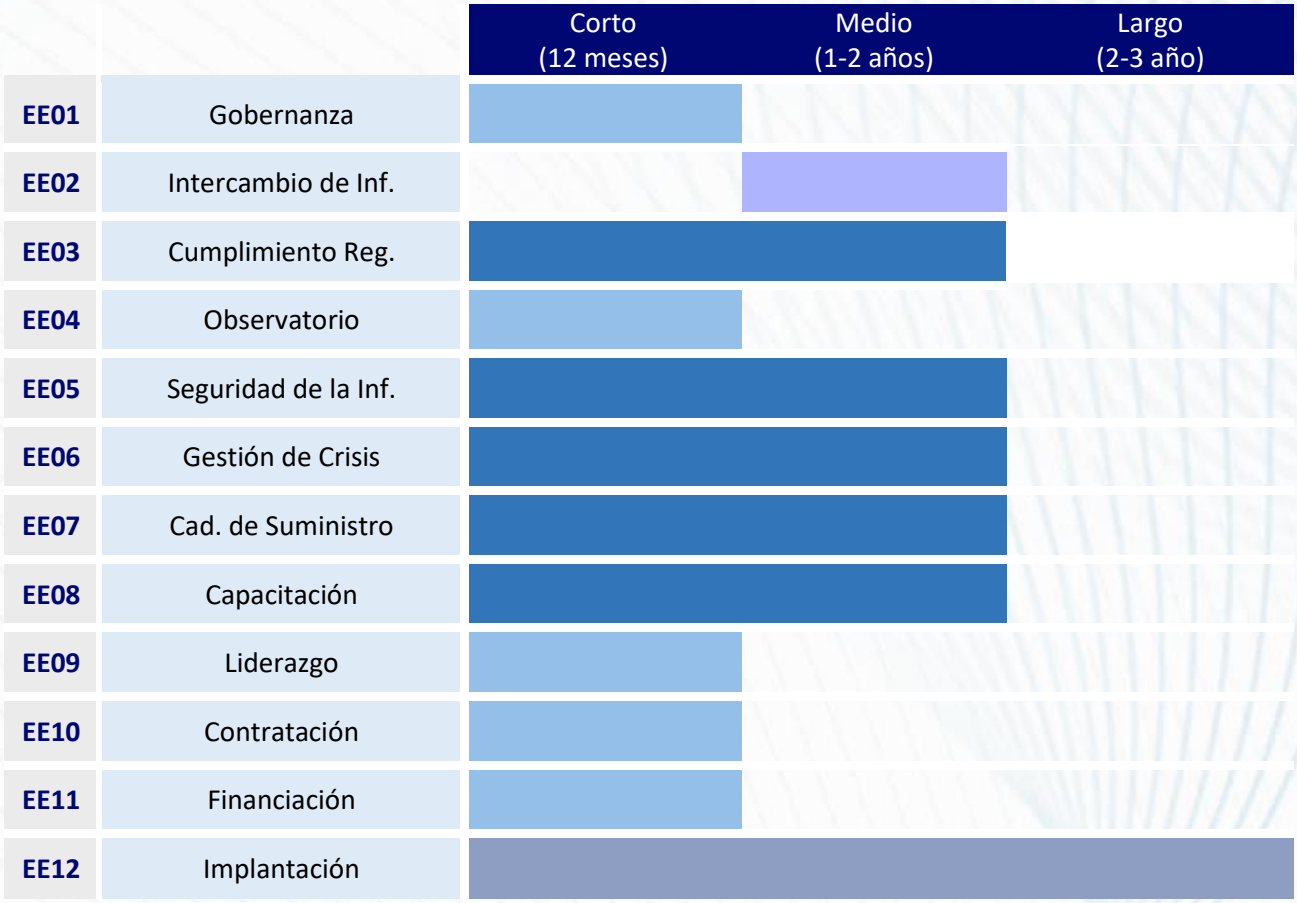
5.1 Mapeo de ejes estratégicos y objetivos

Cada eje estratégico está alineado con uno o más objetivos, asegurando que las iniciativas implementadas contribuyan directamente a los resultados deseados:



5.2 Hoja de ruta

Se ha establecido una hoja de ruta para el despliegue de todos los ejes estratégicos que conforman esta estrategia, asegurando su adecuada implementación. El desarrollo de esta hoja de ruta asentará los pasos específicos y los plazos necesarios para alcanzar los objetivos estratégicos de ciberseguridad del Sistema Nacional de Salud (SNS). A través de un enfoque coordinado y meticuloso, el SNS se prepara para enfrentar los desafíos cibernéticos actuales y futuros, fortaleciendo así la confianza de la ciudadanía en nuestro sistema de salud.



6 Gobernanza de la estrategia de ciberseguridad

6. Gobernanza de la estrategia de ciberseguridad

La gobernanza de la Estrategia de Ciberseguridad del Sistema Nacional de Salud (SNS) se estructura en un modelo de relación que contempla tres niveles jerárquicos: el **Comité Estratégico, el Comité Operativo y el Comité Técnico**. Cada uno de estos comités desempeña un papel crucial en la supervisión de la implantación de la estrategia, asegurando que se alineen los objetivos de ciberseguridad con las necesidades del SNS y se mantenga un enfoque coordinado entre el Ministerio de Sanidad y las Comunidades Autónomas.

Un modelo de gobernanza integral para la Estrategia de Ciberseguridad del Sistema Nacional de Salud que asegure la colaboración entre el Ministerio de Sanidad y las Comunidades Autónomas.

El **Comité Estratégico** está compuesto por representantes de la Dirección del Ministerio de Sanidad y de las Comunidades Autónomas que co-lideran la iniciativa. Este comité tiene la responsabilidad de tomar decisiones estratégicas sobre la implantación de la Estrategia. Su función principal es definir las directrices y prioridades a largo plazo, así como asegurar que la estrategia se integre de manera efectiva en el SNS. Adicionalmente, el Comité Estratégico es el encargado de evaluar el impacto de las decisiones tomadas y de realizar ajustes necesarios en función de la evolución del entorno de ciberseguridad.

El **Comité Operativo** cuenta con representación del Ministerio de Sanidad y de las Comunidades Autónomas co-líderes de la iniciativa. Su finalidad es llevar a cabo un seguimiento táctico de la implantación de la estrategia, así como definir el modelo de relación con terceros (DSN, CCN, INCIBE, etc.). Este comité se encarga de coordinar y supervisar el progreso de las iniciativas en curso. Adicionalmente, tiene la responsabilidad de identificar y resolver problemas operativos que puedan surgir durante la implantación, garantizando que las actividades se realicen de acuerdo con los plazos y objetivos establecidos.

El **Comité Técnico** está conformado por representantes del Ministerio de Sanidad y de todas las Comunidades Autónomas. Su función es realizar un seguimiento continuo de la implantación de la Estrategia de Ciberseguridad y la identificación de posibles desviaciones. Este comité se centra en los aspectos técnicos y operativos de la estrategia, analizando datos y métricas relevantes para evaluar la efectividad de las medidas implementadas. Asimismo, es responsable de proponer mejoras y ajustes técnicos que optimicen la ciberseguridad del SNS.

La estructura de gobernanza de la Estrategia de Ciberseguridad del SNS, a través de estos tres comités, garantiza un enfoque integral y coordinado en la gestión de la ciberseguridad.

7 Anexos

Alinear la estrategia de Ciberseguridad con la Estrategia Nacional de Ciberseguridad, garantiza un mismo rumbo y objetivo común.

7. Anexo I – Relación con Estrategia Nacional de Ciberseguridad

La Estrategia de Ciberseguridad del Sistema Nacional de Salud emana directamente de la Estrategia Nacional de Ciberseguridad, aprobada por el Consejo de Seguridad Nacional, en su reunión del día 12 de abril de 2019. Como no podía ser de otra forma, esta conexión establece una relación directa entre los objetivos estratégicos de ambas iniciativas. A continuación, se identifican y analizan estas interrelaciones, lo que permite garantizar que las acciones y políticas implementadas en el ámbito de la salud se alineen con los principios y directrices establecidos a nivel nacional. De este modo, se promueve un enfoque integral y coordinado que fortalece la ciberseguridad en el sector salud y contribuya a la resiliencia del sistema en su conjunto.

La Estrategia Nacional de Ciberseguridad pivota sobre los siguientes cinco objetivos estratégicos:

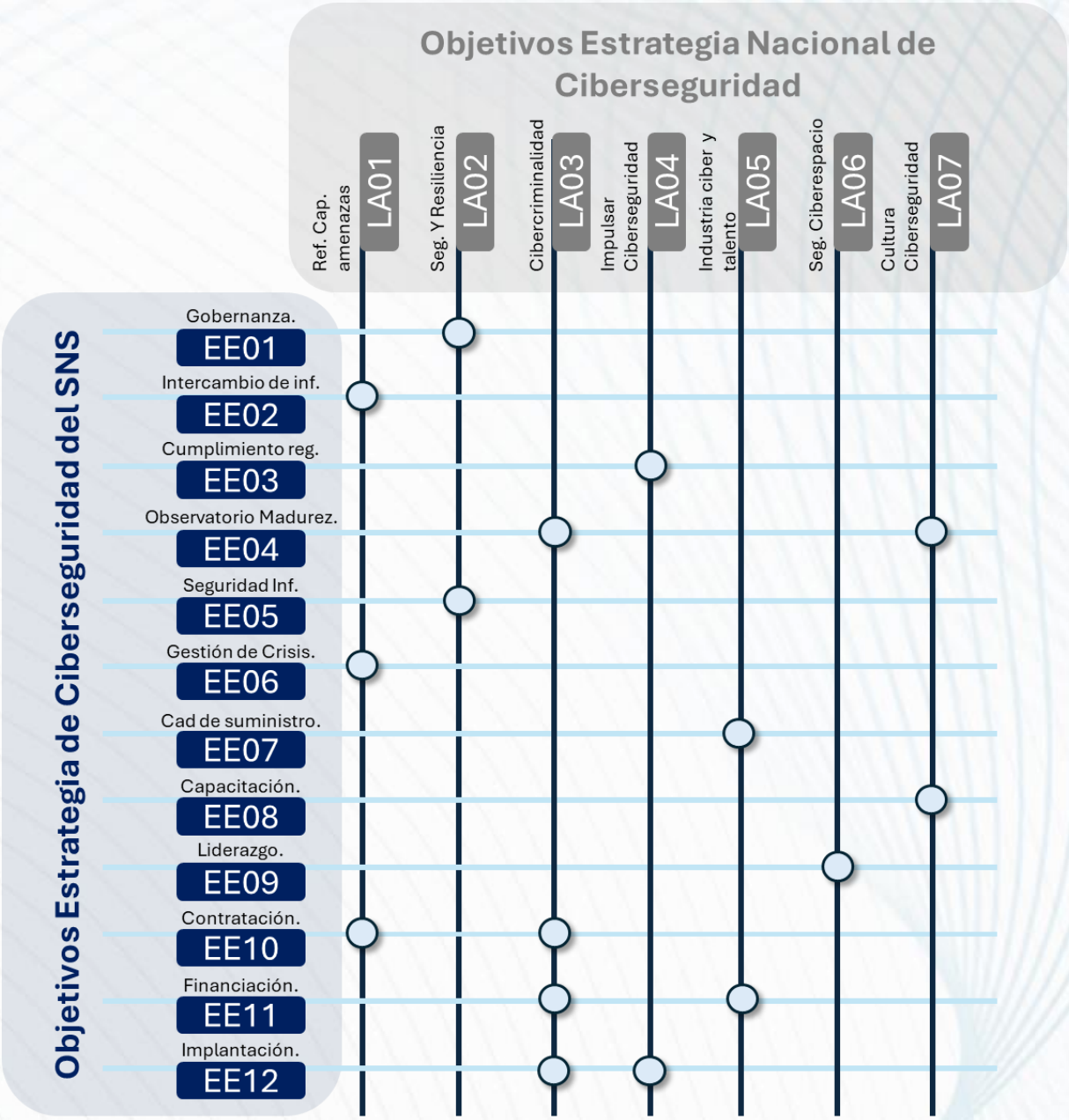
1 Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.	*Se busca consolidar un marco nacional que garantice la protección de la información manejada por el sector público y los servicios esenciales, así como de las redes que los soportan.*
2 Uso seguro y fiable del ciberespacio frente a un uso ilícito o malicioso.	*Asegurar que el ciberespacio sea utilizado de manera segura y confiable, evitando actividades maliciosas e ilícitas.*
3 Protección del ecosistema empresarial y social de los ciudadanos.	*Proteger el entorno empresarial y social de los ciudadanos, asegurando que el ciberespacio sea un lugar seguro para el desarrollo económico y social.*
4 Cultura y compromiso con la ciberseguridad y protección de las capacidades humanas y tecnológicas.	*Fomentar una cultura de ciberseguridad y potenciar las capacidades humanas y tecnológicas necesarias para enfrentar los desafíos de la ciberseguridad.*
5 Seguridad del ciberespacio en el ámbito internacional.	*Promover la seguridad del ciberespacio a nivel internacional, apoyando un ciberespacio abierto, plural, seguro y confiable en apoyo de los intereses nacionales.*

A continuación, se ilustra el mapeo de los objetivos estratégicos de la Estrategia de Ciberseguridad del SNS con los objetivos estratégicos de la Estrategia nacional de Ciberseguridad:

Por otro lado, la Estrategia Nacional de Ciberseguridad desarrolla las siguientes siete líneas de actuación:

1	• Reforzar las capacidades ante las amenazas del ciberespacio. • Mejorar la capacidad de respuesta ante amenazas cibernéticas.
2	• Garantizar la seguridad y resiliencia de los activos estratégicos para España. • Proteger los activos estratégicos del país contra ciberataques.
3	• Reforzar las capacidades de investigación y persecución de la cibercriminalidad. • Mejorar la investigación y persecución de delitos cibernéticos para proteger al ciudadano.
4	• Impulsar la ciberseguridad de ciudadanos y empresas. • Mejorar la seguridad cibernética para individuos y empresas
5	• Potenciar la industria española de ciberseguridad y la generación y retención de talento. • Fortalecer la industria nacional de ciberseguridad y fomentar el talento en este campo.
6	• Contribuir a la seguridad del ciberespacio en el ámbito internacional • Promover un ciberespacio seguro y confiable a nivel internacional
7	• Desarrollar una cultura de ciberseguridad. • Fomentar una cultura de ciberseguridad en la sociedad.

A continuación, se muestra el mapeo de los 12 ejes estratégicos de la Estrategia de Ciberseguridad del SNS con las 7 líneas de actuación de la Estrategia Nacional de Ciberseguridad:



Cabe destacar que existe una interconexión fundamental entre ambas iniciativas. La Estrategia de Ciberseguridad del SNS se desarrolla a partir de los principios y directrices establecidos en la Estrategia Nacional, adaptándose y complementándose con las necesidades específicas del Sistema Nacional de Salud. Este enfoque garantiza que las medidas implementadas no solo se alinean con los objetivos nacionales, sino que también responden a los desafíos únicos que enfrenta el ámbito de la salud en el contexto digital. El mapeo realizado entre las líneas de acción de ambas estrategias evidencia una coherencia y una sinergia que fortalecen la ciberseguridad en el SNS, asegurando así la protección de la información crítica y la continuidad de los servicios esenciales. Este alineamiento no solo es crucial para la resiliencia del sistema de salud, sino que también contribuye a la creación de un entorno más seguro y confiable para todos los ciudadanos.