Estrategia de Ciberseguridad del SNS

NOEMÍ CÍVICOS VILLA.

DG SALUD DIGITAL Y SISTEMAS DE INFORMACIÓN PARA EL SNS.

ENERO 2026

GOBIERNO DE ESPAÑA MINISTERIO DE SANIDAD

Estrategia de Salud Digital

1. Contexto
2. Elaboración
3. Objetivos y ejes estratégicos
4. Conclusiones

https://www.sanidad.gob.es/areas/saludDigital/doc/20250701_Estrategia_de_Ciberseguridad_del_SNS_vF2.pdf

1. Contexto: Importancia creciente de la ciberseguridad

La **digitalización** ha transformado profundamente la atención sanitaria, mejorando la eficiencia y el acceso a la información, pero también **ha incrementado significativamente los riesgos y desafíos en materia de ciberseguridad**

25 de los 215 incidentes notificados por los Estados miembros de la UE en el sector sanitario son en España (2021-Q1'2023)

54% de los incidentes reportados por los Estados miembros de la UE en el sector sanitario son de ransomware (2021-Q1'2023).

¿Quién está detrás de los ciberataques y por qué?

Principales actores:

- **60%** cibercriminales
- **7%** hacktivistas

Motivación:

- **10%** ideológica
- **83%** económica

Una historia clínica puede valer hasta **1.000€** en el mercado negro

¿Cómo nos ciberatacan?

28% Filtraciones de datos

Acceso no autorizado a historiales clínicos y datos sensibles de pacientes, provocado por errores humanos, vulnerabilidades o accesos indebidos.

45% Ransomware

Malware que bloquea el acceso a sistemas hospitalarios o cifra información sanitaria, exigiendo un rescate para su recuperación o para evitar su publicación.

¿Cuáles son las principales causas de los ciberataques?

- **68%** Mala configuración de seguridad
- **16%** Errores humanos
- **4%** Ingeniería social
- **2,5%** Vulnerabilidades en la cadena de suministros

Falta de cultura en seguridad

Falta de inversión en seguridad

¿Qué consecuencias tiene un ciberataque?

- **Seguridad del paciente**: retrasos en tratamientos, falta de acceso a historiales médicos en emergencias….
- **Continuidad asistencial**: imposibilidad de acceder a sistemas críticos.
- **Económico**: elevados costes de recuperación.
- **Reputacional**: pérdida de confianza en ciudadanos.

Fuente: ENISA Thread Landscape: Health Sector, July 2023

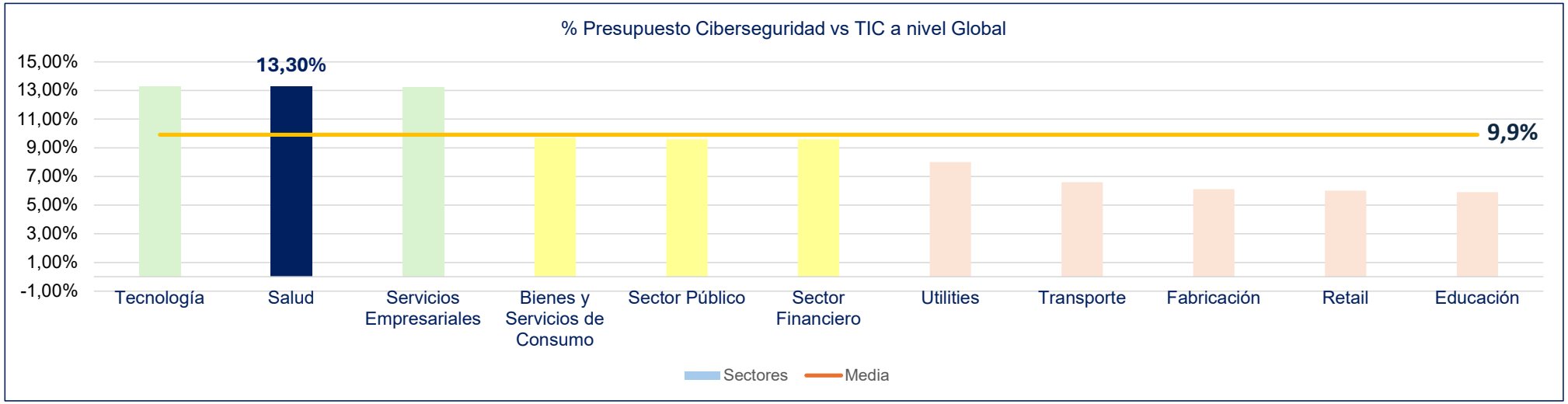
1. Contexto: Presupuesto Ciberseguridad

El sector salud concentra el 8% de los incidentes de ciberseguridad en España, superando a sectores como banca (6%), transporte (6%) y energía (4%).

La inversión en ciberseguridad en los Servicios de Salud en España está por debajo de la media global para el sector

9,4% ha sido la **Inversión Ciberseguridad** sobre presupuesto TIC en la Sanidad Pública durante el **2024**

Fuente: Índice SEIS 2024



Fuente: IANS & Artico, Security Budget Benchmark Summary Report, 2022

2. Elaboración de la Estrategia de Ciberseguridad del SNS

El proceso

Trabajo colaborativo e iterativo entre el Ministerio de Sanidad, las CCAA y el INGESA.

Participación en foros y eventos de la COM sobre implicaciones de Ciberseguridad en Salud y Hospitales.

Análisis del estado de la ciberseguridad en los distintos Servicios de Salud.

Estrategia alineada con el CCN.

Estrategia informada al Consejo Nacional de Ciberseguridad.

Las premisas

Alineamiento estratégico

- Estrategia de Salud Digital
- Estrategia Nacional de Ciberseguridad
- Plan de Acción europeo ciberseguridad hospitales y los prestadores de asistencia sanitaria

- **Complementariedad con iniciativas estatales y autonómicas**
- **Cumplimiento normativo:** ENS, LOPDGDD, LPIC, Reglamento EEDS...

GT 1.1 CIBERAP

Grupo inicial encargado de colaborar en la elaboración de la estrategia nacional de ciberseguridad para el SNS, cuyo antecedente es el GT del mismo nombre del Plan de Transformación Digital de AP (ESD y PERTE para la salud de vanguardia).

Análisis de las prioridades actuales

- Cumplimiento normativo
- Intercambio temprano información incidentes
- Riesgos en dispositivos médicos y tecnologías emergentes
- Seguridad de cadena de suministros
- Protección de la información de salud
- Indicadores de madurez
- Formación

El resultado

Estrategia **única y específica** para todo el SNS, consensuada y alineada con las necesidades y prioridades de los Servicios de Salud y el Ministerio de Sanidad

Participantes

Todos los Servicios Públicos de Salud de las CCAA e INGESA, y el Ministerio de Sanidad como ente coordinador para guiar y supervisar la implementación:

Ministerio de Sanidad

Andalucía, Aragón, Canarias, Cantabria, Castilla La Mancha, Castilla y León, Cataluña, INGESA, Comunidad de Madrid, Comunidad Foral de Navarra, Comunidad Valenciana, Extremadura, Galicia, Islas Baleares, La Rioja, País Vasco, Principado de Asturias, Región de Murcia

* Co-Líderes del proyecto

Elementos

8 Objetivos Estratégicos

12 Ejes Estratégicos de Actuación

34 Programas Únicos de Trabajo

Fortalecimiento de la protección de datos y la integridad de los servicios sanitarios.

Seguridad al paciente y garantizar la **continuidad asistencial.**

Cumplimiento y alineamiento con los requerimientos Europeos

APROBADA POR EL PLENO DEL CISNS EN NOVIEMBRE DE 2025

3. Objetivos

Establecer una red de colaboración en ciberseguridad:

Mejorando la detección, respuesta y resiliencia del SNS ante ciberataques.

Posicionar al SNS como un referente de ciberseguridad:

Tanto a nivel nacional y europeo, promoviendo mejores prácticas.

Establecer indicadores:

Desarrollar métricas para evaluar la madurez en ciberseguridad y detectar áreas de mejora.

Garantizar la continuidad asistencial:

Reforzando la resiliencia operativa y la cadena de suministros.

Definir medidas:

Asegurar la integridad, confidencialidad y accesibilidad de los datos sanitarios, garantizando su trazabilidad y autenticidad.

Fomentar el cumplimiento normativo:

Promoviendo un entorno seguro.

Impulsar la investigación y el análisis de riesgos:

Para anticipar y mitigar amenazas.

Promover la capacitación continua:

Asegurando que todos los actores del SNS estén preparados para identificar y responder a ciber amenazas

3. Ejes estratégicos

Estrategia Ciberseguridad ECSNS

Misión

Funciones

Alcance

Objetivos estratégicos

Ejes estratégicos

Implementación progresiva en 3 años

- LA1. Gobernanza de la ciberseguridad Sanitaria.
- LA2. Intercambio de Información de ciberseguridad.
- LA3. Cumplimiento regulatorio en ciberseguridad.
- LA4. Observatorio de madurez en ciberseguridad.
- LA5. Seguridad de la información del SNS.
- LA6. Modelo de Gestión de Crisis.
- LA7. Gestión de la Cadena de Suministros.
- LA8. Mejora de la capacitación en ciberseguridad.
- LA9. Liderazgo de pensamiento en ciberseguridad.
- LA10. Optimizar el proceso de contratación de productos y servicios de ciberseguridad
- LA11. Búsqueda de líneas de financiación.
- LA12. Apoyo para la implantación de la estrategia en los servicios públicos de salud.

5. Conclusiones

La ciberseguridad es cosa de todos:

Consejo Interterritorial
SISTEMA NACIONAL DE SALUD

GOBIERNO DE ESPAÑA
MINISTERIO DE SANIDAD

Servicios de Salud

CCN-CERT
centro criptológico nacional

Responsabilidad de la dirección

La **regulación** en materia de **ciberseguridad establece** que los **órganos de dirección** de los **servicios** de **salud serán responsables** de **aplicar** las **medidas** para la **gestión** de **riesgos** de **ciberseguridad**, de **supervisar** su implantación efectiva y **asumirán** la **responsabilidad** por su incumplimiento, mediante las correspondientes **actuaciones disciplinarias**. (*Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad*)

Cambio Cultural

Para asegurar una adecuada protección en ciberseguridad del SNS se requiere promover un cambio cultural en los Servicios de Salud.

Dedicación del Equipo

La elevada implicación y participación de los equipos de seguridad de los Servicios Salud ha sido fundamental para la definición de la ECSNS y lo seguirá siendo para su adecuada implantación.

Inversión en Personal

Incrementar la ciberseguridad del SNS pasa por la inversión en personal con cualificación específica en ciberseguridad en los Servicios de Salud.

Inversión Económica

Incrementar la ciberseguridad del SNS para por una inversión económica en los Servicios de Salud para la implementación de medidas técnicas de ciberseguridad.

¡Gracias!