Consejo de la Unión Europea

Bruselas, 16 de enero de 2025
(OR. en)

5426/25

CYBER 21
SAN 15

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	15 de enero de 2025
A:	D.ª Thérèse BLANCHET, secretaria general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2025) 10 final
Asunto:	COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES Plan de Acción europeo sobre la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria

Adjunto se remite a las delegaciones el documento COM(2025) 10 final.

Adj.: COM(2025) 10 final

COMISIÓN
EUROPEA

Bruselas, 15.1.2025
COM(2025) 10 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

Plan de Acción europeo sobre la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria

1. Introducción

El entorno de seguridad de la UE está cambiando rápidamente, mientras se intensifican los ataques híbridos y los ciberataques cuyo objetivo es desestabilizar nuestra sociedad, buscando divisiones y perturbaciones, así como beneficiarse de la ciberdelincuencia. Por este motivo, Europa debe reforzar urgentemente su preparación y resiliencia frente a esta nueva realidad, en todos los sectores y en consonancia con un enfoque que implique a todas las instancias de la Administración y a todos los sectores de la sociedad, tal como se pide en el informe del asesor especial de la presidenta de la Comisión Europea, Sauli Niinistö.

Los sistemas sanitarios seguros y resilientes son una piedra angular del modelo social de la UE. Sin embargo, tanto los hospitales como los sistemas sanitarios se enfrentan a crecientes amenazas, en particular por parte de las bandas que utilizan programas de secuestro de archivos con fines lucrativos, impulsadas por el alto valor de los datos de los pacientes, incluidos los historiales médicos digitales. De hecho, el sector sanitario se ha convertido en la industria más atacada en la UE en los últimos cuatro años, en particular durante la pandemia de COVID-19, durante la cual las infraestructuras sanitarias fueron cada vez más objeto de ciberataques. Los ciberataques contra hospitales y prestadores de asistencia sanitaria causan daños directos a las personas, retrasan los procedimientos médicos, colapsan las salas de emergencia y, en casos extremos, podrían dar lugar a la pérdida de vidas humanas.

A medida que el sector se va adentrando en una vital transformación digital, cada vez son mayores los riesgos. La sanidad digital y el uso y la reutilización de los datos sanitarios pueden permitir modelos de asistencia más adaptados a las necesidades y preferencias de las personas y de los pacientes, al prevenir la aparición de enfermedades o permitir un tratamiento más temprano. La integración de herramientas y soluciones digitales en los procesos clínicos, así como el uso y la reutilización de los datos sanitarios, pueden servir de base para la mejora de las decisiones clínicas y contribuir a la automatización de la salud, así como a una atención al paciente mejor y más rápida. Las herramientas digitales, el uso de datos y los productos sanitarios, que a menudo están conectados a internet e impulsados por la inteligencia artificial (IA), son fundamentales para abordar retos como la escasez de profesionales sanitarios.

Al mismo tiempo, las herramientas digitales también amplían los objetivos potenciales de los ciberdelincuentes. Además, determinados agentes estatales no dudan en atacar los centros sanitarios, como demuestra la actual guerra de agresión de Rusia contra Ucrania. Esto convierte al sector en un posible objetivo de ciberataques como parte de una campaña híbrida más amplia. Estos ciberataques no solo ponen en peligro la seguridad de los pacientes, sino que también erosionan la confianza de los ciudadanos en las infraestructuras sanitarias y conllevan importantes costes de recuperación. Más allá de la vigilancia contra los ciberataques, una infraestructura digital resiliente y segura también es esencial para apoyar la aplicación y la plena implantación del Espacio Europeo de Datos de Salud [1] (EEDS).

Por lo tanto, ha llegado el momento de mejorar y reforzar la ciberseguridad y la resiliencia de los hospitales y los prestadores de asistencia sanitaria de Europa, como destacó la presidenta Von der Leyen en sus orientaciones políticas para la Comisión 2024-2029[2]. Este Plan de Acción responde a la urgencia

[1] https://www.consilium.europa.eu/es/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/

[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_es

de la situación y a las amenazas únicas a las que se enfrenta el sector. No existe un «remedio milagroso» para los retos en materia de ciberseguridad a los que se enfrentan los sistemas sanitarios. En su lugar, el Plan de Acción aboga por reforzar la prevención, la preparación y un enfoque más coordinado de la solidaridad, aprovechando al mismo tiempo los conocimientos de los expertos en la industria europea de la ciberseguridad. Como tal, el Plan de Acción refleja el enfoque de la UE en materia de seguridad, que se seguirá desarrollando y formalizando en la próxima Estrategia Europea de Seguridad Interior, definiendo una respuesta global para hacer frente a todas las amenazas a la seguridad interior y centrándose en la capacidad de anticipar las amenazas, prevenir los daños y proteger a las personas, actuando a todos los niveles con un enfoque que implique a todos los sectores de la sociedad.

El sector sanitario incluye un gran número de entidades y agentes, como hospitales, clínicas, residencias, centros de rehabilitación y diversos prestadores de asistencia sanitaria, junto con la industria farmacéutica, médica y biotecnológica, los fabricantes de productos sanitarios y los institutos de investigación sanitaria. Este Plan de Acción se centra principalmente en la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria, entendidos como tales cualquier persona física o jurídica, o cualquier otra entidad, que proporcione legalmente asistencia sanitaria en el territorio de un Estado miembro[3]. Los hospitales y los prestadores de asistencia sanitaria son interdependientes con otras entidades sanitarias y son los más cercanos a las personas. Al mismo tiempo, las medidas para mejorar la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria deberían también abordar los riesgos que afectan a la cadena de suministro y su ecosistema en general, derivados, por ejemplo, de entidades que utilizan datos sanitarios para la investigación y el aprendizaje automático o que fabrican productos sanitarios, en particular productos sanitarios basados en tecnologías digitales que se conectan a internet u otros dispositivos («internet de las cosas»).

Si bien la protección de los sistemas sanitarios es principalmente una competencia nacional, la salud es también un sector crítico en el marco de la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (SRI 2)[4]. Los ciberdelincuentes y otros agentes de riesgo operan a través de las fronteras, y los retos en materia de ciberseguridad a los que se enfrentan las organizaciones sanitarias también son similares en todos los Estados miembros. La cooperación a escala europea es valiosa para compartir y estimular las mejores prácticas nacionales y de la UE. Por ello, el Plan de Acción propone un mecanismo de coordinación y otras medidas a escala de la UE, al tiempo que pide a los Estados miembros que emprendan acciones para marcar la diferencia en la asistencia sanitaria y en el ecosistema sanitario en general.

El Plan de Acción se centra en desarrollar las capacidades del sector para **prevenir** incidentes de ciberseguridad en primer lugar, ya que más vale siempre prevenir que curar. En segundo lugar, el Plan de Acción detalla medidas para mejorar el intercambio de información sobre ciberseguridad y la capacidad para **detectar** ciberamenazas, permitiendo una reacción más rápida. En tercer lugar, ofrece

[3] Artículo 3, letra g), de la Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32011L0024

[4] 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 (Directiva SRI 2),https://eur-lex.europa.eu/eli/dir/2022/2555

medidas para **responder** mejor a los incidentes y **recuperarse** de ellos. Por último, el Plan de Acción prevé formas de **disuadir** a los agentes de riesgo de lanzar ataques contra los sistemas sanitarios en Europa.

El Plan de Acción se ejecutará en estrecha colaboración con los prestadores de asistencia sanitaria y el ecosistema sanitario en general, los Estados miembros y la comunidad de ciberseguridad. Es fundamental aplicar un enfoque más colaborativo para seguir definiendo y perfeccionando las acciones con mayor repercusión, de modo que todos los prestadores esenciales de asistencia sanitaria de Europa puedan beneficiarse de ellas. Por lo tanto, la presente Comunicación irá acompañada de la puesta en marcha de una consulta exhaustiva con las partes interesadas, el sector y los Estados miembros. La cooperación internacional es importante para la ciberseguridad debido a la naturaleza carente de fronteras e interconectada de las ciberamenazas. También existen amenazas de ciberseguridad comparables en los países candidatos y vecinos, así como en otros países que son socios estratégicos de la UE. En última instancia, esto puede poner en peligro la seguridad de las infraestructuras críticas en la UE. Por ello, será importante reflejar las enseñanzas que se extraigan de la aplicación del Plan de Acción también en la cooperación de la UE tanto con los países candidatos como con otros países socios, habida cuenta de los niveles de amenaza a los que están expuestos, respectivamente.

2. Reto para la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria

Ciberamenazas para el sector sanitario

Los ciberataques están aumentando a escala mundial y dentro de la UE, con un panorama de amenazas cada vez más complejo y dinámico. Los avances en la IA están dotando a los delincuentes y otros agentes malintencionados de herramientas potentes para aumentar la precisión y el impacto de sus operaciones, y remodelando las posibilidades de ciberdefensa, permitiendo una acción automatizada y en tiempo real contra los ataques.

Los programas de secuestro de archivos siguen presentando un reto crítico en materia de ciberseguridad en la UE y en todo el mundo; hay un informe que estima que su coste anual mundial superará los 250 000 millones EUR de aquí a 2031[5]. Cuando los delincuentes atacan con programas de secuestro, no solo cifran los datos de las víctimas para exigir un rescate, sino que filtran cada vez más información delicada para ejercer una presión adicional. Otro reto destacado son las vulnerabilidades de los programas y equipos informáticos: según la Agencia de la Unión Europea para la Ciberseguridad (ENISA)[6], la asistencia sanitaria es el sector que declaró el mayor número de incidentes de seguridad relacionados con

[5] Cybersecurity Ventures (1 de junio de 2024): *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031* («Se prevé que los costes mundiales de los daños provocados por programas de secuestro de archivos superen los 265 000 millones USD para 2031», publicación solamente disponible en inglés). Disponible en https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

[6] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento sobre la Ciberseguridad»), https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

dichas vulnerabilidades.[7] Otras amenazas crecientes incluyen los ataques distribuidos de denegación de servicios, diseñados para desbordar un sistema específico con una inundación de tráfico, lo que lo hace inaccesible para los usuarios legítimos[8].

El sector sanitario se enfrenta a tendencias similares de amenazas a la ciberseguridad, con un énfasis pronunciado en los ataques con programas de secuestro de archivos. Según la ENISA, los programas de secuestro de archivos representaron el 54 % de los incidentes de ciberseguridad analizados en el sector sanitario en el período 2021-2023. El 83 % de los ataques estaban motivados por fines económicos, impulsados por el elevado valor de los datos sanitarios, mientras que el 10 % de los ataques tenían una motivación ideológica[9]. Del mismo modo, un informe de la Comisión de 2024 constató que el 71 % de los ataques con efectos en la atención a los pacientes, como el tratamiento o el diagnóstico tardío y las dificultades de acceso a los servicios de emergencia, fueron secuestro de archivos[10]. Los ataques con programas de secuestro de archivos pueden tener un efecto especialmente disruptivo en la provisión de servicios sanitarios, poniendo en peligro la seguridad de los pacientes. Además, estos ataques suelen ir acompañados de violaciones de la seguridad de los datos de los pacientes[11], que a menudo incluyen información delicada relacionada con la salud y violan el derecho fundamental de las personas a la protección de sus datos personales.

Al mismo tiempo, con la creciente digitalización de la asistencia sanitaria, la superficie de ataque está aumentando. Según el Informe sobre el estado de la Década Digital 2024, una media del 79 % de los ciudadanos de la UE tiene acceso en línea a sus historiales médicos digitales de atención primaria[12]. Los historiales médicos digitales, los sistemas de información clínica, los sistemas de flujo de trabajo hospitalario, los sistemas informáticos para la gestión del reembolso de tratamientos, los sistemas de imagenología médica y los productos sanitarios utilizados con fines de diagnóstico o de seguimiento de los pacientes son ejemplos de herramientas digitales que pueden desempeñar un papel importante en el fomento de la eficiencia y el rendimiento del sector sanitario, pero que también son objetivos potenciales de ataques a la ciberseguridad. Determinadas actividades sanitarias, como los cuidados intensivos y la radiología, o ciertos ámbitos médicos como la oncología y la cardiología, que dependen en gran medida de productos sanitarios basados en tecnologías digitales, son particularmente vulnerables al riesgo de ciberataques. Además, los problemas relacionados con la cadena de suministro pueden dar lugar a la

[7] Panorama de amenazas de ENISA: Sector sanitario (julio de 2023).
[8] Panorama de amenazas de ENISA 2024.
[9] Panorama de amenazas de ENISA: Sector sanitario (julio de 2023). El informe presentó un análisis de los proveedores de asistencia, así como de otros tipos de organizaciones, incluidas las organizaciones que llevan a cabo investigaciones relacionadas con la salud, las entidades que fabrican determinados productos relacionados con la salud, las autoridades sanitarias, las organizaciones de seguros de enfermedad, las instalaciones residenciales de tratamiento y los prestadores de servicios sociales. Disponible en https://www.enisa.europa.eu/publications/health-threat-landscape
[10] Comisión Europea: Centro Común de Investigación, Reina, V. y Griesinger, C.: *Cyber security in the health and medicine sector — A study on available evidence of patient health consequences from cyber incidents in healthcare settings,* («La ciberseguridad en el sector de la salud y la medicina: estudio sobre las pruebas disponibles de las consecuencias sanitarias para los pacientes resultantes de incidentes cibernéticos en entornos sanitarios», documento en inglés), Oficina de Publicaciones de la UE, 2024, https://op.europa.eu/es/publication-detail/-/publication/9d3355cf-591f-11ef-acbc-01aa75ed71a1
[11] Según el panorama de amenazas de ENISA para el sector sanitario, se confirmó la violación de la seguridad o el robo de datos en el 43 % de los incidentes de programas de secuestro analizados.
[12] Informe sobre el estado de la Década Digital 2024

adquisición de productos sanitarios con una ciberseguridad insuficiente, lo que agrava los riesgos generales existentes.

Por ejemplo, durante la pandemia de COVID-19, un ataque con programas de secuestro de archivos paralizó gran parte del sistema sanitario irlandés, lo que dio lugar a la cancelación parcial de servicios en 31 de los 54 hospitales de agudos durante la mañana del incidente.[13] Los servicios sanitarios tuvieron que retomar los registros en papel, lo que ralentizó la eficiencia de las operaciones. El ataque tuvo su origen en un correo electrónico de *phishing* o ataque por suplantación de identidad que contenía un archivo malicioso adjunto.[14] El incidente demostró el potencial de propagación de los ciberataques por diferentes sistemas y, en consecuencia, la importancia de proteger la totalidad de la superficie de ataque de toda organización sanitaria. También subrayó la importancia de garantizar una cultura esencial de ciberhigiene y ciberseguridad en todas las organizaciones.

Madurez de la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria

El panorama de la asistencia sanitaria en la UE es muy diverso, ya que la titularidad, estructura y tamaño de los hospitales y otros prestadores de asistencia sanitaria varían considerablemente entre los distintos Estados miembros. En algunos casos, la gobernanza de la asistencia sanitaria se basa en un enfoque centralizado a nivel nacional; en otros, a nivel regional y local; los prestadores de asistencia sanitaria pueden ser públicos o privados. Además, también pueden existir diferencias dentro de un mismo país, por ejemplo, cuando existen importantes disparidades socioeconómicas y territoriales entre regiones, lo que da lugar a un panorama complejo. El funcionamiento de este complejo panorama sanitario puede verse amenazado por importantes crisis sanitarias, debido a enfermedades transmisibles —como la pandemia de COVID-19— pero también a otros riesgos para la salud, como por ejemplo los relacionados con el cambio climático. Por último, se observa una considerable variabilidad y fragmentación del nivel de digitalización y adopción de tecnología por parte de los prestadores de asistencia sanitaria. Un ejemplo de esta complejidad es que la interrupción del servicio provocada por un incidente de ciberseguridad puede causar daños y perjuicios graves a los pacientes incluso en instalaciones sanitarias a pequeña escala, entre ellas las clínicas o servicios médicos de emergencia que prestan un servicio esencial a un número relativamente bajo de usuarios.

Según el Informe de ENISA de 2024 sobre el estado de la ciberseguridad en la Unión[15], la madurez de la ciberseguridad del sector sanitario de la UE es moderada y existen grandes diferencias en cuanto a este nivel de madurez entre las distintas entidades sanitarias de toda Europa. Pueden observarse carencias en ámbitos clave como la suficiencia de recursos humanos, los conocimientos de las organizaciones sobre sus cadenas de suministro de tecnologías de la información y comunicación (TIC) y la instalación de elementos de seguridad actualizados en los productos. El sector atraviesa dificultades para garantizar

[13] Dirección del Servicio de Salud irlandés (2021): «Ciberataque de Conti contra el Servicio de Salud irlandés: análisis independiente tras el incidente».
[14] Dirección del Servicio de Salud irlandés: «Ciberataque y respuesta del Servicio de Salud irlandés». Disponible en hhttps://www2.hse.ie/services/cyber-attack/what-happened/.
[15] ENISA: Informe de 2024 sobre el estado de la ciberseguridad en la Unión (septiembre de 2024). Disponible en https://www.enisa.europa.eu/publications/health-threat-landscape

un nivel básico de ciberhigiene y unas medidas fundamentales de seguridad, como demuestra el hecho de que casi todas las organizaciones sanitarias encuestadas se enfrentan a retos a la hora de realizar evaluaciones de riesgos de ciberseguridad, mientras que casi la mitad de ellas nunca ha realizado un análisis de riesgos.[16]

Otro reto importante para la ciberseguridad de los hospitales es la intersección de la tecnología de la información (TI) y la tecnología operativa (OT), en la que confluyen distintas prioridades de seguridad en cuanto a confidencialidad, disponibilidad y fiabilidad, y una infracción en un ámbito puede afectar al otro. El Informe de ENISA de 2024 sobre el estado de la ciberseguridad en la Unión subraya además que el sector sanitario no está funcionando adecuadamente a la hora de garantizar la seguridad de los productos y procesos de TIC que utiliza, debido a la gran variedad de entidades, dispositivos y productos sanitarios.

Esta diversidad, junto con la existencia de distintos niveles de concienciación sobre ciberseguridad entre el personal y la dirección de los hospitales, crea un complejo reto para garantizar la ciberseguridad de los sistemas sanitarios. Por ejemplo, según el Eurobarómetro de 2024 sobre cibercapacidades, solo el 25 % de las empresas encuestadas del sector de la salud, la educación y la asistencia social había impartido actividades de formación o de sensibilización sobre ciberseguridad en los 12 meses anteriores[17]. Es necesario actuar para fomentar una cultura de sensibilización en materia de ciberseguridad entre los profesionales sanitarios de primera línea. Por ejemplo, las rotaciones del personal, el uso de estaciones de trabajo compartidas, la mala gestión de la autenticación y el uso de soportes extraíbles suponen fuentes adicionales de vulnerabilidad que afectan a la ciberseguridad de los prestadores de asistencia sanitaria[18].

En muchos casos, la tecnología de la información y la tecnología operativa se externalizan, al menos en parte. El Eurobarómetro de 2024 constató que el porcentaje de empresas que externalizan al menos algunos aspectos de su ciberseguridad es el mayor en el sector de la salud, la educación y la asistencia social, y que el 57 % de las empresas encuestadas lo hacen[19]. Del mismo modo, existe una fuerte tendencia a migrar a la computación en la nube, impulsada por la necesidad de un almacenamiento y una gestión de datos expansibles, la rentabilidad, la mejora de la colaboración y el apoyo a tecnologías avanzadas como la IA y el internet de las cosas médicas. En 2022, el 58 % de las organizaciones sanitarias utilizaron una plataforma de salud digital en la nube[20]. Sin embargo, aunque este cambio puede aportar importantes mejoras del rendimiento, también conlleva riesgos que requieren decisiones informadas sobre la adjudicación de los contratos y una configuración segura.

---

[16] Panorama de amenazas de ENISA: Sector sanitario (julio de 2023). Disponible en https://www.enisa.europa.eu/publications/health-threat-landscape

[17] Flash Eurobarómetro 547 sobre cibercapacidades (mayo de 2024). Disponible en https://europa.eu/eurobarometer/surveys/detail/3176

[18] Panacea: ciberseguridad centrada en las personas en la asistencia sanitaria (2021): Libro Blanco: enseñanzas extraídas de PANACEA sobre la ciberprotección de hospitales y centros asistenciales.

[19] Flash Eurobarómetro 547 sobre cibercapacidades (mayo de 2024). Disponible en https://europa.eu/eurobarometer/surveys/detail/3176

[20] ENISA: Informe de 2022 sobre las inversiones de SRI (noviembre de 2022). Disponible en https://www.enisa.europa.eu/publications/nis-investments-2022

Por encima de todos estos desafíos está la cuestión del desarrollo de capacidades y la financiación. La financiación de la ciberseguridad en el sector sanitario siempre ha sido insuficiente y sigue constituyendo un desafío universal en la UE[21]. Además, estos retos de financiación surgen en el contexto del envejecimiento de la población, que se espera ejerza presiones presupuestarias generalizadas sobre los sistemas sanitarios europeos en las próximas décadas.

El uso continuado de herramientas obsoletas y sistemas heredados, los limitados recursos para prevenir incidentes o reaccionar ante ellos y las lagunas en la madurez de la ciberseguridad se derivan a menudo de carencias de financiación. Los hospitales se enfrentan al desafío constante de equilibrar el mantenimiento de una infraestructura digital y segura actualizada con otras inversiones necesarias para mejorar la atención a los pacientes, como la contratación de médicos y otros profesionales sanitarios, la aplicación de nuevos métodos de diagnóstico y tratamiento y la adquisición de productos. Según ENISA[22], el sector sanitario ocupa solo el 7.º puesto de los 12 sectores estudiados en lo que se refiere a la proporción del gasto en seguridad de la información con respecto al gasto total en TI, siendo el 8,3 % la mediana dentro del sector sanitario.

3. Centro Europeo de Apoyo a la Ciberseguridad para hospitales y prestadores de asistencia sanitaria

El marco de ciberseguridad de la UE ofrece una amplia gama de herramientas que deben aprovecharse para mejorar la seguridad y la resiliencia de los hospitales y los prestadores de asistencia sanitaria. Para hacer frente a los numerosos retos señalados anteriormente, es necesario desarrollar un enfoque estratégico unificado a escala de la UE, que reúna los recursos, los conocimientos especializados y las herramientas necesarias para hacer frente a las ciberamenazas eficazmente. Una visión global, así como una mejor planificación y coordinación, son esenciales para ayudar a los prestadores de asistencia sanitaria de toda la UE a reforzar sus defensas. Para lograrlo, ENISA es la entidad más indicada para establecer, dentro de su organización, un **Centro Europeo de Apoyo a la Ciberseguridad para hospitales y prestadores de asistencia sanitaria**[23], como parte de su mandato[24] de salvaguardar y apoyar las infraestructuras críticas de la UE.

El Centro de Apoyo debe **desarrollar progresivamente un amplio catálogo de servicios que atienda las necesidades de los hospitales y los prestadores de asistencia sanitaria**, en el que se describa la gama de servicios disponibles para la preparación, la prevención, la detección y la respuesta. En colaboración con las autoridades de los Estados miembros y aprovechando la experiencia de los hospitales y los prestadores de asistencia sanitaria, el Centro de Apoyo debe desarrollar un repositorio

[21] La organización y prestación de servicios sanitarios y atención médica es una competencia nacional en virtud del artículo 168 del Tratado de Funcionamiento de la Unión Europea, y la financiación de los sistemas sanitarios varía de un Estado miembro a otro.

[22] ENISA: Informe de 2022 sobre las inversiones en SRI (noviembre de 2022). Disponible en https://www.enisa.europa.eu/publications/nis-investments-2022

[23] En este documento, se utiliza indistintamente la denominación larga con su abreviatura «Centro de Apoyo».

[24] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») (DO L 151 de 7.6.2019, p. 15).

fácil de utilizar y fácilmente accesible que contenga todos los instrumentos disponibles a escala europea, nacional y regional. Al llevar a cabo sus actividades, debe garantizar una coordinación adecuada con los Estados miembros y apoyar la priorización y la ejecución de las acciones necesarias en tiempo real.

Como elemento fundamental para el desarrollo del catálogo de servicios del Centro de Apoyo, la Comisión propondrá la puesta en marcha de proyectos piloto en toda la UE para desarrollar mejores prácticas en materia de ciberhigiene y evaluación de riesgos para la seguridad, así como para abordar la necesidad de un seguimiento continuo de la ciberseguridad, la inteligencia frente a amenazas y la respuesta a incidentes utilizando soluciones de ciberseguridad de última generación. Los resultados de estos proyectos piloto, que se financiarán con cargo al programa Europa Digital, ejecutado por el Centro Europeo de Competencia en Ciberseguridad (ECCC, por sus siglas en ingles), servirán de base para otras acciones a escala de la UE, incluido el trabajo del Centro de Apoyo.

Gráfico 1: Conceptos para el catálogo de servicios del Centro de Apoyo para hospitales y prestadores de asistencia sanitaria

3.1. Prevención de incidentes de ciberseguridad

Acciones sencillas que alteran las probabilidades

Las medidas básicas de ciberseguridad, como garantizar que los sistemas estén actualizados, gestionar copias de seguridad y aplicar la autenticación multifactor, pueden, según una estimación, proteger a las organizaciones de hasta el 98 % de los ataques[25]. Muchas de las medidas de ciberhigiene y gestión de riesgos con mayor impacto son relativamente sencillas de adoptar, lo que las convierte en herramientas fácilmente accesibles para mejorar la ciberseguridad. Por lo tanto, una de las funciones clave del Centro de Apoyo debe ser **elaborar orientaciones claras y específicas que destaquen las prácticas de ciberseguridad más críticas y ayuden a los prestadores de asistencia sanitaria a aplicarlas**. Este apoyo debe extenderse más allá de los grandes hospitales para incluir asesoramiento personalizado a entidades más pequeñas, como las consultas de los médicos generalistas locales y las clínicas especializadas, que a menudo carecen de recursos para incluir equipos específicos de ciberseguridad, pero que siguen siendo igualmente vulnerables a los ataques. Además, es necesario tener en cuenta la importancia regional de las determinadas entidades sanitarias para garantizar la atención a los pacientes, por ejemplo, en las zonas escasamente pobladas. Los institutos de investigación sanitaria que manejan grandes cantidades de datos personales delicados también podrían beneficiarse de recibir orientaciones sobre medidas básicas de ciberseguridad para aumentar su resiliencia.

Las organizaciones sanitarias también están sujetas a una serie de obligaciones relacionadas con la ciberseguridad derivadas de la legislación de la UE[26]. Si bien las obligaciones son cruciales para

[25] Informe de protección digital de Microsoft de 2022. Disponible en https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[26] Como la Directiva SRI 2; el Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (Reglamento de Ciberresiliencia), https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R2847https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R2847; el Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32017R0745(Reglamento de productos sanitarios); el Reglamento (UE) 2017/746 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios para diagnóstico *in vitro* (Reglamento de productos sanitarios para diagnóstico *in vitro*)https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32017R0746; el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679; el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial), https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689, y la propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre el Espacio Europeo de Datos Sanitarios, COM/2022/197 final, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52022PC0197. Las negociaciones concluyeron con un

garantizar una rigurosa base de referencia común para la ciberseguridad y la seguridad de los datos, es esencial garantizar que el panorama normativo no sea innecesariamente complicado y engorroso. La atención especial al cumplimiento de las normas no debe contrarrestar el objetivo de fomentar una sólida cultura de ciberseguridad. Un **catálogo normativo de fácil acceso puede ayudar a minimizar la carga administrativa para las entidades sujetas a múltiples instrumentos reguladores**. Además de dedicarse al desarrollo de orientaciones y herramientas, el Centro de Apoyo debe colaborar estrechamente con la Comisión y los Estados miembros para desarrollar y difundir dicho catálogo lo antes posible. Por lo tanto, el Centro de Apoyo desempeñaría un papel importante a la hora de simplificar la comprensión y la aplicación de las normas de ciberseguridad, por ejemplo proporcionando directrices[27] sobre la aplicación y, en caso necesario, promoviendo los estándares pertinentes.

Las próximas **carteras europeas de identidad digital** son otra herramienta para facilitar la aplicación sencilla de buenas prácticas de ciberhigiene. Reducir la dependencia respecto de mecanismos de identificación frágiles, como las contraseñas, es esencial para mitigar los riesgos de acceso no autorizado a los datos sanitarios. Es fundamental la transición hacia sistemas de inicio de sesión basados en una identificación fiable. La cartera de identidad digital de la UE ofrece un enfoque armonizado, a escala de la UE, para la identificación electrónica de los profesionales sanitarios, proporcionando una solución sólida y unificada para finales de 2026. Todos los sistemas de información sanitaria en línea necesarios para implantar la autenticación reforzada de usuario estarán obligados a aceptar la cartera a efectos de identificación a partir de finales de 2027[28].

Preparación y apoyo específico

Las pruebas de preparación, que implican acciones como las pruebas de penetración, son una piedra angular de una ciberseguridad eficaz, y la Comisión ya ha asignado financiación a ENISA para iniciativas piloto de preparación, lo que revela que el sector sanitario se encuentra entre los ámbitos más demandados para la realización de pruebas y evaluaciones adicionales a fin de detectar lagunas en la madurez de la ciberseguridad. Con la entrada en vigor de la Ley de Cibersolidaridad, estos esfuerzos se ampliarán significativamente, dirigidos por el ECCC. Para hacer frente a esta necesidad, la Comisión propondrá, en consulta con el Grupo de Cooperación SRI, CyCLONe[29] y ENISA, identificar la salud como un sector susceptible de apoyo mediante las **pruebas coordinadas de preparación** en el marco de la Ley de Cibersolidaridad. Además, el Centro de Apoyo debe desarrollar un **marco de evaluación de la madurez de la ciberseguridad específico para la asistencia sanitaria**. Estas evaluaciones de la madurez proporcionarían a las entidades información viable sobre sus vulnerabilidades, al tiempo que les permitirían demostrar su preparación en materia de ciberseguridad a los pacientes y las partes interesadas, generando confianza en sus servicios. A nivel agregado, el Centro de Apoyo debe llevar a

acuerdo político en la primavera de 2024 y, una vez finalizadas, la publicación en el Diario Oficial está prevista para la primavera de 2025.

[27] La elaboración de directrices sobre la interpretación del Reglamento General de Protección de Datos (RGPD) es responsabilidad del Comité Europeo de Protección de Datos (CEPD). La elaboración de orientaciones por parte de ENISA debe respetar plenamente las prerrogativas del CEPD.

[28] artículo 5 *septies*, apartados 1 y 2, del Reglamento (UE) n.º 910/2014.

[29] Red europea de organizaciones de enlace para las crisis de ciberseguridad

cabo una **evaluación anual de la madurez cibernética sanitaria**, que establecería una visión clara de la ciberseguridad del sector sanitario tanto a escala nacional como de la UE.

El sector sanitario depende en gran medida de contratistas externos para los servicios de ciberseguridad[30], lo que pone de relieve la necesidad de un apoyo específico para reforzar las defensas. Aprovechando el éxito de iniciativas como los bonos de innovación de la UE, los **Estados miembros deben considerar medidas específicas, como los bonos de ciberseguridad para los hospitales y prestadores de asistencia sanitaria muy pequeños, pequeños y medianos**. Estos bonos proporcionarían asistencia financiera para poner en marcha medidas específicas de ciberseguridad. La priorización de la asignación de bonos debe basarse en los resultados de las pruebas de preparación y las evaluaciones de madurez.

Los conocimientos y el contexto locales son cruciales para el despliegue efectivo de bonos u otros programas de apoyo, garantizando su pertinencia y accesibilidad. Los fondos de la UE, como el Fondo Europeo de Desarrollo Regional, ya participan activamente en el apoyo a las iniciativas en materia de ciberseguridad y salud digital, por lo que podrían servir de vehículo para desarrollar sistemas de bonos de ciberseguridad específicos para los prestadores de asistencia sanitaria. Para impulsar este esfuerzo, el Centro de Apoyo colaboraría con los Estados miembros y las autoridades encargadas de los programas a nivel regional para apoyar el desarrollo de estos sistemas de bonos regionales, aprovechando las lecciones extraídas de los proyectos nacionales existentes, así como de las acciones financiadas en el marco del Programa Europa Digital, a fin de garantizar una aplicación práctica y con impacto.

Además, desde 2014, los programas Horizonte han desempeñado un papel decisivo en la financiación de una serie de iniciativas de investigación centradas en mejorar la resiliencia de las instituciones sanitarias, como los hospitales, frente a las ciberamenazas y en mitigar los riesgos asociados al uso indebido de las tecnologías emergentes. Los resultados concretos incluyen una serie de herramientas, marcos y sistemas especializados, como las herramientas de evaluación de riesgos, las plataformas de intercambio de datos que preservan la privacidad, las soluciones criptográficas, los programas de formación en materia de sensibilización sobre la ciberseguridad y los sistemas de detección de amenazas en tiempo real. En particular, estas soluciones se han validado rigurosamente a través de aplicaciones piloto reales en entornos sanitarios, lo que garantiza su eficacia y su aplicabilidad práctica en la protección contra las ciberamenazas.

Asegurar las cadenas de suministro en el ámbito de la asistencia sanitaria

Un reto clave para las organizaciones sanitarias lo supone la gestión de las cadenas de suministro de TIC complejas, que incluyen una serie de productos como los productos sanitarios conectados, los sistemas de historiales clínicos digitales y los equipos informáticos de oficina. Los hospitales y los prestadores de asistencia sanitaria necesitan sistemas y servicios de TIC fiables y seguros para sus operaciones. Para ayudar a abordar los retos en materia de ciberseguridad en el sector sanitario, el Grupo de Cooperación SRI debe llevar a cabo una **evaluación coordinada de los riesgos para la seguridad, estudiando los**

[30] Véase el Informe de 2023 sobre las inversiones en SRI de ENISA (noviembre de 2023), en el que se destaca la prominencia del apoyo externo para la auditoría y el cumplimiento de la ciberseguridad. Disponible en https://www.enisa.europa.eu/publications/nis-investments-2023

riesgos tanto técnicos como estratégicos relacionados con las cadenas de suministro de productos sanitarios y proponiendo medidas para mitigarlos.[31] Según proceda, el Grupo de Cooperación SRI debe colaborar con el Grupo de Coordinación de Productos Sanitarios.

La Ley de Ciberresiliencia es un nuevo marco integral que establece requisitos de ciberseguridad para las fases de planificación, diseño y desarrollo, así como para el tratamiento, la reparación y la notificación de vulnerabilidades aprovechadas activamente en relación con casi todos los programas y equipos informáticos, en cada etapa de la cadena de valor[32]. Los productos médicos son un tipo de producto utilizado en uno de los ámbitos más delicados de nuestra sociedad. Los requisitos de ciberseguridad para estos productos se derivan del Reglamento sobre los productos sanitarios y del Reglamento sobre los productos sanitarios para diagnóstico *in vitro*[33]. La evaluación en curso de dichos Reglamentos está examinando el potencial de aumentar la coherencia y las sinergias entre estos marcos con el fin de garantizar la simplificación y una ciberseguridad de última generación.

Además, las conclusiones de la evaluación de riesgos deberían ayudar a las organizaciones sanitarias a revisar las prácticas de ciberseguridad de su cadena de suministro, tal como exige la Directiva SRI 2, y podrían servir de base para la elaboración de nuevas **directrices de contratación pública**[34]. Elaboradas por la ENISA a través de su Centro de Apoyo, estas directrices deben reflejar las tendencias recientes, como la migración a la nube del almacenamiento de datos de los pacientes, e incluir la necesidad de una migración segura de los datos sanitarios electrónicos a entornos en la nube. Además, las nuevas directrices deben ofrecer herramientas prácticas para que las organizaciones lleven un seguimiento de sus cadenas de suministro, incluidos los proveedores de servicios de seguridad gestionados, los informes de certificación o las evaluaciones de riesgos de terceros.

En el caso de la nube, es necesario adoptar nuevas medidas para abordar los retos particulares de la gestión de datos sanitarios delicados, incluidos el aumento de la seguridad, la privacidad y los riesgos operativos. Para reforzar las salvaguardias, los expertos recomiendan integrar la «seguridad por defecto y desde el diseño» en los servicios en la nube. Este enfoque da prioridad a las infraestructuras seguras, a la gestión proactiva de las vulnerabilidades y a una combinación de soluciones públicas y privadas para la nube. El seguimiento continuo y la utilización de certificaciones específicas para cada prestador, como las certificaciones de los prestadores de seguridad, y las auditorías de cumplimiento de las normas nacionales e internacionales, también son esenciales para garantizar unas prácticas de seguridad sólidas.

En el caso de servicios como IcS (infraestructura como servicio), PcS (plataforma como servicio) y ScS (software como servicio), la aplicación de las medidas de seguridad suele recaer en el cliente. Sin

[31] A tenor del artículo 22 de la Directiva SRI 2.
[32] En una primera fase, a partir del 1 de agosto de 2025, se exigirá a las categorías generales de equipos radioeléctricos que no entren en el ámbito de aplicación del Reglamento sobre los productos sanitarios y del Reglamento sobre los productos sanitarios para diagnóstico *in vitro* que cumplan los requisitos esenciales de la Directiva sobre equipos radioeléctricos relacionados con la ciberseguridad cuando se introduzcan en el mercado único. En una segunda fase, a partir del 11 de diciembre de 2027, comenzará a aplicarse la Ley de Ciberresiliencia.
[33] En diciembre de 2019, el Grupo de Coordinación de Productos Sanitarios publicó orientaciones sobre la ciberseguridad de los productos sanitarios, apoyando a los fabricantes en el cumplimiento de los requisitos del anexo I de los dos Reglamentos: https://ec.europa.eu/docsroom/documents/41863?locale=es.
[34] Sobre la base de las Directrices de la ENISA sobre contratación pública para la ciberseguridad en los hospitales de 2020 (febrero de 2020). Disponible en https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

embargo, muchas organizaciones sanitarias carecen de los recursos necesarios para satisfacer estos requisitos de forma independiente. Para hacer frente a esta situación, **debe alentarse a los prestadores de servicios en la nube a que apliquen las medidas de seguridad de referencia como atributo estándar**. Estas medidas reducirían el riesgo de configuraciones erróneas, mantendrían una protección coherente en todos los entornos gestionados por el cliente y ofrecerían mayores garantías a los usuarios. El establecimiento de una base de referencia de seguridad por defecto tendría por objeto equilibrar la solidez de la protección con su viabilidad, garantizando la facilidad de uso para una amplia gama de organizaciones sanitarias. Este esfuerzo implicaría una estrecha colaboración entre los proveedores de servicios en la nube y el sector sanitario, aprovechando las mejores prácticas de la industria para crear soluciones eficaces y expansibles.

Formación y desarrollo de capacidades

Disponer de una mano de obra con capacidades demandadas es importante para el crecimiento sostenible a largo plazo y la competitividad en Europa, así como para unos servicios de alta calidad, incluidos los servicios sanitarios. La escasez de profesionales cualificados en ciberseguridad es un reto importante en toda Europa, con un déficit estimado de 299 000 profesionales para cubrir las necesidades de mano de obra en la UE[35]. Según el Eurobarómetro de 2024 sobre cibercapacidades[36], el 81 % de las empresas considera que las dificultades para contratar personal de ciberseguridad suponen un riesgo importante de posibles ciberataques. En los sectores de la educación, la salud y el trabajo social, el 66 % de los puestos en el ámbito de la ciberseguridad están cubiertos por empleados que proceden de puestos no relacionados con este ámbito, lo que pone de relieve la necesidad urgente de reciclaje y perfeccionamiento profesionales.

Para hacer frente a este reto, el Centro de Apoyo debe colaborar con el futuro Consorcio de Infraestructuras Digitales Europeas (EDIC) para cibercapacidades previsto en la Comunicación de la Comisión sobre la Academia de Capacidades en Ciberseguridad[37]. El trabajo debe facilitar los intercambios entre los profesionales de la ciberseguridad del sector sanitario, como los responsables centrales de seguridad informática (CISO). Una posible acción sería crear una **red europea de directores de seguridad de la información (CISO) en el ámbito de la salud**, empezando por una reserva de expertos para compartir y desarrollar mejores prácticas, estrategias de retención del talento y soluciones para atraer a profesionales de la ciberseguridad al sector sanitario. Además, en el marco de la Academia de Capacidades en materia de Ciberseguridad, deben desarrollarse recursos para ampliar la mano de obra especializada en ciberseguridad en el sector sanitario con el apoyo de la industria y el

[35] Panorama de la ciberseguridad de 2024:Conocimientos extraídos del estudio sobre la mano de obra en el ámbito de la ciberseguridad | Plataforma de capacidades y empleos digitales
[36] Flash Eurobarómetro 547 sobre cibercapacidades
[37] Comunicación de la Comisión al Parlamento Europeo y al Consejo: Colmar la brecha de talento en materia de ciberseguridad para impulsar la competitividad, el crecimiento y la resiliencia de la UE («Academia de Capacidades en materia de Ciberseguridad»). COM(2023) 207 final.

mundo académico. A este respecto, debe alentarse a las partes interesadas del sector a que se comprometan a apoyar la mejora de la formación en materia de ciberseguridad.

El error humano sigue siendo uno de los principales factores que contribuyen a los incidentes de ciberseguridad en la asistencia sanitaria, lo que pone de relieve la necesidad crítica de la formación integral del personal y de la concienciación sobre cuestiones cibernéticas. Dado el uso frecuente de herramientas digitales por parte de los profesionales sanitarios, es fundamental dotarlos de conocimientos sobre prácticas seguras. Las campañas de formación y sensibilización específicas pueden reducir significativamente los riesgos. Para abordar esta cuestión, el Centro de Apoyo debe trabajar con los profesionales y los prestadores de servicios sanitarios, y cooperar con los prestadores de educación y formación, el sector, el Consorcio de Infraestructuras Digitales Europeas (EDIC) para las capacidades en materia de ciberseguridad y las autoridades de los Estados miembros a fin de crear y difundir **módulos y cursos de formación en línea amplios y de fácil acceso**.

La incorporación de módulos de competencia digital y ciberseguridad en los planes de estudios es crucial para crear una base sólida de ciberseguridad en la asistencia sanitaria. Estos módulos deben abordar cuestiones propias de este sector como la protección de datos de los pacientes y las vulnerabilidades que afectan a la seguridad de los productos sanitarios. El desarrollo de estos recursos debe tener en cuenta acciones previas, como el proyecto BeWell financiado en el marco del programa Erasmus +[38] y el proyecto PANACEA financiado en el marco de Horizonte 2020[39].

3.2. Capacidades europeas para la detección de ciberamenazas contra el sector sanitario

La detección eficaz de ciberamenazas es esencial para responder rápidamente a los incidentes. Los agentes de riesgo tienen a su alcance técnicas para dificultar la detección de las intrusiones, lo que les permite prolongar los períodos de acceso no permitido a un sistema[40]. Por lo tanto, unas mejores capacidades de detección de amenazas pueden ayudar a frenar en seco los ciberataques. Por ejemplo, en el ataque con programas de secuestro contra el prestador finlandés de servicios de psicoterapia Vastaamo, durante el cual el autor extorsionó a pacientes a quienes había robado sus historiales médicos confidenciales, la intrusión inicial se produjo en 2018, pero el prestador no tuvo conocimiento de ello hasta 2020[41].

El intercambio de información y la colaboración eficientes son esenciales para mejorar la detección de amenazas y la conciencia situacional en toda la UE. Los equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés) desempeñan un papel fundamental a la hora de recibir

[38] BeWell: alianza del sector sanitario para una futura estrategia de capacitación digital y ecológica de su personal sanitario sobre capacidades digitales y ecológicas. Disponible en https://bewell project.eu/.
[39] Panacea — Protección y privAcidad de las iNfraestructuras hospitalarias y sanitarias con herrAmientas inteligentes de Ciberseguridad y protección frente a las cibEramenazas para dAtos y personas. Disponible en https://cordis.europa.eu/project/id/826293/es.
[40] Panorama de amenazas de ENISA 2023.
[41] Decisión 1150/161/2021 del Defensor del Pueblo finlandés en materia de protección de datos.

notificaciones de incidentes, cuasi incidentes y posibles amenazas, y de ofrecer información sobre las medidas de mitigación a escala nacional. No obstante, **se anima encarecidamente a los Estados miembros a que también comuniquen todas las notificaciones de ciberincidentes procedentes de hospitales y prestadores de asistencia sanitaria al Centro de Apoyo de ENISA para hacer posible la conciencia situacional en la UE**. Idealmente, esto debe ir acompañado de una caracterización significativa de las distintas dimensiones pertinentes de los incidentes, incluidas las vulnerabilidades profundas ya conocidas y el impacto en los servicios sanitarios, con los consiguientes efectos adversos para los pacientes. Además, se anima a los fabricantes de productos sanitarios y de diagnóstico *in vitro* a notificar voluntariamente, a través de la plataforma única de notificación que establecerá y gestionará la ENISA en el marco de la Ley de Ciberresiliencia, las vulnerabilidades que están siendo activamente aprovechadas o los ciberincidentes graves que afecten a la seguridad de estos productos, así como, potencialmente, otras vulnerabilidades, incidentes, cuasi incidentes o ciberamenazas que puedan afectar al perfil de riesgo de estos productos.

Cuando la información contenida en los informes ya no sea delicada, el Centro de Apoyo podría crear un catálogo europeo de vulnerabilidades conocidas que están siendo aprovechadas patrocinado por ENISA para productos sanitarios, sistemas de historiales clínicos digitales y proveedores de equipos y programas informáticos en el ámbito de la salud. Para hacer frente a los retos significativos de la detección de amenazas, el Centro de Apoyo debe introducir un **servicio de suscripción de alerta temprana a escala de la UE para el sector sanitario, que proporcione alertas casi en tiempo real**. Este servicio se serviría de los datos tratados por los CSIRT, las entidades y los fabricantes del ámbito sanitario, los servicios de inteligencia de fuentes abiertas (OSINT, por sus siglas en inglés) y otros agentes pertinentes, como los ISAC y las autoridades policiales. Una mayor cooperación entre ENISA y la Agencia de la Unión Europea para la Cooperación Policial (Europol), por ejemplo en lo que respecta a los patrones de ciberdelincuencia contra el sector sanitario, impulsaría aún más la conciencia situacional.

Los ISAC sirven de recursos centrales para la inteligencia sobre ciberamenazas, fomentando el intercambio de información bidireccional entre los sectores público y privado y promoviendo la confianza. El Centro de Apoyo debe intensificar la asistencia al **ISAC sanitario europeo** con herramientas e intercambio de información e informes sectoriales de conciencia situacional, así como mediante el fomento de una comunidad de confianza para la colaboración táctica y estratégica. Los Estados miembros deben promover el desarrollo de los ISAC sanitarios nacionales[42]. También debe alentarse a los ISAC a que reúnan a los prestadores de asistencia sanitaria con los fabricantes para dar lugar a una comprensión común de las amenazas a la ciberseguridad, incluidas las que afectan a la cadena de suministro, y a facilitar el diálogo sobre un diseño seguro de los productos que tenga realmente en cuenta las realidades de la aplicación sobre el terreno.

[42] Por ejemplo, Finlandia tiene un ISAC nacional para el sector del bienestar social y la asistencia sanitaria. Véase el Centro Nacional de Ciberseguridad de Finlandia: «grupos de intercambio de información del ISAC», disponible en https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

3.3.Respuesta rápida y recuperación

Dada la gran sensibilidad de los datos sanitarios de los pacientes y los efectos potencialmente devastadores de los ciberataques en los servicios sanitarios, una respuesta rápida y eficaz a los incidentes de ciberseguridad es crucial para salvaguardar la seguridad de los pacientes. Cuando un hospital o un prestador de asistencia sanitaria se enfrenta a un ciberataque, el primer punto de contacto es el CSIRT nacional pertinente[43]. El CSIRT es responsable de prestar apoyo en tiempo oportuno, idealmente en un plazo de 24 horas, para ayudar a gestionar incidentes significativos. Sin embargo, si un incidente supera la capacidad del CSIRT, debe disponerse de apoyo de la UE para garantizar una respuesta rápida y eficaz.

La Reserva de Ciberseguridad de la UE, creada en virtud de la Ley de Cibersolidaridad, presta servicios de respuesta a incidentes de seguridad por parte de prestadores de seguridad gestionados de confianza para ayudar en incidentes de ciberseguridad significativos o a gran escala y en los esfuerzos de recuperación iniciales. Esta reserva está diseñada para complementar los esfuerzos de los CSIRT de los Estados miembros, permitiéndoles solicitar apoyo adicional en casos relacionados con sectores críticos como la salud. Para mejorar este sistema, la **Comisión y la ENISA deben garantizar que la Reserva incluya un servicio de respuesta rápida específico para el sector sanitario.** En complementariedad con otros marcos existentes, este servicio desplegaría expertos para gestionar sin demora incidentes de ciberseguridad significativos o a gran escala en los sistemas de asistencia sanitaria cuando el apoyo nacional sea insuficiente.

Para mejorar la respuesta y la recuperación, el Centro de Apoyo, en colaboración con el Grupo de Cooperación SRI, la red de CSIRT y, en su caso, Europol, debe elaborar **manuales de respuesta a incidentes cibernéticos adaptados a la asistencia sanitaria**. Estos manuales orientarían tanto a los CSIRT como a las organizaciones sanitarias a la hora de responder a amenazas específicas de ciberseguridad, incluidos los programas de secuestro de archivos. Dada la importancia de una cooperación eficaz entre los CSIRT y las autoridades encargadas de hacer cumplir la ley en la respuesta e investigación de incidentes de ciberseguridad de carácter delictivo, los manuales de actuación deben proporcionar, entre otros aspectos, orientaciones claras sobre la notificación de tales incidentes a estas autoridades. Además, el Centro de Apoyo podría **facilitar un amplio despliegue de ejercicios nacionales de ciberseguridad, aprovechando las experiencias de ejercicios como el Cyber Europe 2022 de ENISA, para poner a prueba los manuales de actuación y reforzar los protocolos de respuesta a incidentes.**

Para fundamentar las políticas y evaluar la eficacia de las medidas adoptadas contra los ataques con programas de secuestro, es necesario recopilar más datos. A tal efecto, los Estados miembros deben solicitar a las entidades sujetas a la Directiva SRI 2, incluidas las organizaciones sanitarias, que informen sobre cualquier pago de rescate efectuado o que tengan intención de efectuar, junto con el resto de la información que faciliten al notificar incidentes de ciberseguridad significativos. Esta información ayuda

[43] El artículo 23, apartado 1, de la Directiva SRI 2 establece el requisito de que las entidades esenciales o importantes notifiquen los incidentes significativos al CSIRT pertinente o, en su caso, a la autoridad competente.

a investigar eficazmente los incidentes con programas de secuestro, incluido el rastreo de los pagos en plataformas de intercambio de criptomoneda para identificar a los destinatarios.

La velocidad de recuperación es un factor fundamental para mantener la resiliencia y la confianza pública, en particular en el ámbito de la asistencia sanitaria, donde el tiempo de inactividad puede perturbar la atención a los pacientes. Para una recuperación eficaz tras los ataques con programas de secuestro, los prestadores de asistencia sanitaria deben disponer de copias de seguridad seguras, actualizadas y aisladas que puedan restablecerse rápidamente. Como parte de su catálogo de servicios, el Centro de Apoyo podría ofrecer **un servicio de suscripción para la recuperación de datos tras el secuestro de archivos, ayudando a los hospitales y a los prestadores de asistencia sanitaria a preparar planes de recuperación con antelación.** ENISA y Europol deben colaborar para identificar las cepas más comunes de programas de secuestro dirigidas a las organizaciones sanitarias y **ampliar el repositorio de herramientas de descifrado** disponibles a través del proyecto «No More Ransom» (No más secuestros)[44]. También deben desarrollar y promover orientaciones accesibles para ayudar a los prestadores de asistencia sanitaria a evitar el pago de rescates mediante el uso de herramientas de descifrado.

La **Iniciativa Internacional contra los Programas de Secuestro de Archivos**[45] es un valioso espacio para el intercambio de información sobre incidentes específicos de programas de secuestro, así como para el desarrollo de las capacidades de los países miembros para reforzar sus marcos de ciberseguridad y para llevar a cabo su labor de investigación contra los agentes de programas de secuestro. La Comisión, en colaboración con la alta representante, seguirá impulsando la cooperación en la Iniciativa de lucha contra los programas de secuestro de archivos, en particular contra las amenazas de programas de secuestro en el sector sanitario. Además, la Comisión buscará la cooperación en el **Grupo de Trabajo sobre Ciberseguridad del G7** para reforzar la ciberseguridad del sector sanitario. En particular, el Grupo de Trabajo podría estudiar las posibilidades de apoyar al sector sanitario frente a amenazas como los programas de secuestro, basándose en reflexiones como la Declaración conjunta sobre ataques con programas de secuestro contra instalaciones sanitarias, de 8 de noviembre de 2024, presentada en el contexto del Consejo de Seguridad de las Naciones Unidas[46].

4. Medidas nacionales

La capacidad del presente Plan de Acción para mejorar la ciberseguridad en el sector sanitario depende de la participación y el compromiso activos de los Estados miembros. Para aplicar con éxito el Plan de Acción, los Estados miembros podrían designar **Centros Nacionales de Apoyo a la Ciberseguridad específicos para hospitales y prestadores de asistencia sanitaria.** Estos centros actuarían como puntos de contacto primarios para el sector sanitario a nivel nacional, en estrecha colaboración con el Centro de Apoyo de ENISA. Cuando sea posible y pertinente, los Estados miembros deben designar organismos

[44] https://www.nomoreransom.org/es/index.html.
[45] https://www.counter-ransomware.org/
[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/

ya existentes, como los CSIRT nacionales de salud o las autoridades correspondientes, como Centros Nacionales de Apoyo a la Ciberseguridad.

También se anima a los Estados miembros a crear **planes de acción nacionales centrados en la ciberseguridad en el sector sanitario**. Estos planes describirían los riesgos específicos de ciberseguridad a los que se enfrentan los sistemas sanitarios y las medidas nacionales adoptadas para abordarlos, garantizando al mismo tiempo el uso eficaz de los recursos y las prácticas a escala europea. El Centro de Apoyo de ENISA puede ayudar a desarrollar estos planes, teniendo en cuenta los planes nacionales ya existentes y coordinando los esfuerzos para garantizar que los recursos y las estrategias de los distintos Estados miembros se complementen entre sí.

Otro objetivo clave para los Estados miembros es facilitar el intercambio de recursos entre los prestadores de asistencia sanitaria, lo que podría lograrse mediante la **adquisición conjunta o la puesta en común de recursos** a escala nacional, regional o incluso europea. Este enfoque reduciría la carga financiera de las entidades individuales, aumentando al mismo tiempo su poder de negociación con los proveedores de servicios de ciberseguridad.

Por ejemplo, el programa francés CaRE[47] ha introducido una serie de medidas a nivel nacional y regional para abordar los retos en materia de recursos: un cibercatálogo ofrece una visión general de las soluciones y paquetes cibernéticos puestos a disposición de los hospitales a través de la agencia nacional de ciberseguridad, la agencia digital de salud, las agencias regionales, las organizaciones nacionales de compras y las soluciones comerciales. Esto se complementa con financiación adicional para que las agencias regionales ofrezcan recursos compartidos.

Los Estados miembros también deben abordar los niveles insuficientes de inversión en ciberseguridad en el sector sanitario. Para garantizar una financiación adecuada, deben establecer **parámetros de referencia no vinculantes y hacer un seguimiento de los objetivos de financiación destinados específicamente a la ciberseguridad**, garantizando al mismo tiempo que estas inversiones no vayan en detrimento de la atención esencial de los pacientes. Estos objetivos de financiación también deben tener por objeto integrar los aspectos relativos a la seguridad en todas las inversiones digitales en el sector. Los Estados miembros pueden intercambiar buenas prácticas y asesoramiento sobre estos objetivos a través de plataformas como la red de sanidad electrónica[48].

5. Cooperación entre los sectores público y privado:

La cooperación público-privada y la consulta con los prestadores de asistencia sanitaria, otras entidades del sector sanitario y los agentes pertinentes del sector de la ciberseguridad son esenciales para el éxito de la aplicación del Plan de Acción. Para seguir contribuyendo al trabajo del Centro de Apoyo, la

[47] Agencia digital de salud francesa: Cybersécurité acceleration et Résilience des Établissements (CaRE). Disponible en: https//esante.gouv.fr/strategie-nationale/cybersecurite.

[48] La red de sanidad electrónica es una red voluntaria que conecta a las autoridades nacionales responsables de la sanidad electrónica designadas por los Estados miembros, creada en virtud del artículo 14 de la Directiva 2011/24/UE.

Comisión, respaldada por ENISA, creará un Consejo Consultivo conjunto sobre Ciberseguridad Sanitaria formado por representantes de alto nivel de ambos ámbitos —la asistencia sanitaria y la ciberseguridad—, que podrá asesorar a la Comisión y al Centro de Apoyo sobre medidas de fuerte repercusión y debatir el desarrollo ulterior de asociaciones público-privadas en este ámbito. El Consejo aprovechará los esfuerzos existentes para las asociaciones público-privadas, incluido el ISAC sanitario europeo.

Además, la Comisión pondrá en marcha un **llamamiento a la acción** para que las empresas de ciberseguridad, las fundaciones, las instituciones educativas y las partes interesadas del sector **se comprometan a emprender acciones para abordar los retos de este**. Por ejemplo, basándose en su propia experiencia, la Academia de Cibercapacidades podría comprometerse a impartir cursos de formación y elaborar material enfocado en el sector sanitario para profesionales de la ciberseguridad[49]. Otros compromisos también podrían referirse a las actividades de sensibilización o la prestación de servicios de seguridad gestionados a entidades especialmente vulnerables, de forma gratuita o a un coste reducido, con el fin de mejorar su preparación y resiliencia en materia de ciberseguridad. Además, los compromisos podrían consistir en compartir la inteligencia sobre ciberamenazas con el Centro de Apoyo de ENISA. El Centro de Apoyo debe mantener una visión general de los compromisos contraídos en el marco del llamamiento a la acción, con el objetivo de garantizar su coherencia y complementariedad.

6. Disuasión a los agentes de ciberamenazas

Las políticas internas y externas de ciberseguridad de la UE deben respaldar el objetivo de disuadir a los agentes de ciberamenazas de atacar a los sistemas sanitarios europeos. Los ciberataques contra organizaciones sanitarias son un tipo especialmente inaceptable de ciberactividad malintencionada, dada su capacidad para poner en riesgo la seguridad de los pacientes y la vida humana. Por lo tanto, es necesario emplear con total contundencia la capacidad disuasoria de la Unión en el ámbito de la ciberseguridad y aplicar rigurosamente la ley para socavar el modelo general de negocio de los agentes de amenazas contra el sector sanitario y privarles de beneficios fáciles. Esta actividad incluiría el fomento de las investigaciones transfronterizas mediante un mayor intercambio de indicadores de compromiso y otros datos pertinentes, y una mayor atención a los objetivos de alto valor y a los facilitadores clave de la delincuencia, como los servidores blindados o los servicios de mezcla de criptomonedas.

El **conjunto de instrumentos de ciberdiplomacia** ofrece un marco para prevenir los ciberataques contra la UE, sus Estados miembros y sus socios, desincentivarlos y darles respuesta. La alta representante seguirá utilizando el marco de sanciones contra los ciberataques existente para responder a las amenazas contra los sistemas sanitarios.

Exigir responsabilidades a los agentes delictivos por sus acciones es un importante elemento disuasorio. Por consiguiente, los Estados miembros deben velar por que el control del cumplimiento de la ley esté plenamente integrado en sus planes de acción nacionales. En particular, deben hacer pleno uso de las

[49] Academia de Cibercapacidades¡Participa!Plataforma de capacidades y empleos digitales

disposiciones de la Directiva relativa a los ataques contra los sistemas de información[50] y del Convenio de Budapest sobre la Ciberdelincuencia del Consejo de Europa para disuadir de los ataques, llevar a los delincuentes ante la justicia y desmantelar las infraestructuras delictivas que facilitan estos ataques[51]. La aplicación satisfactoria de estas herramientas debe garantizar que se castiguen las acciones delictivas y malintencionadas contra la asistencia sanitaria.

7. Aplicación y seguimiento del Plan de Acción

A lo largo de este Plan de Acción, se ha previsto una serie de tareas para la creación de un Centro de Apoyo en ENISA. Este enfoque garantiza una aplicación holística y coherente del Plan de Acción, evitando al mismo tiempo la creación de nuevas entidades que den lugar a posibles solapamientos y gastos generales. La Comisión velará por que el Centro de Apoyo cuente con los recursos adecuados.

Una vez que el Centro de Apoyo esté operativo, ENISA, en consulta con la Comisión, deberá proporcionar periódicamente actualizaciones del trabajo del Centro de Apoyo al Consejo de Administración de ENISA, así como a las redes pertinentes de los Estados miembros, en particular el Grupo de Cooperación SRI, la red de CSIRT, la red de sanidad electrónica y, cuando proceda, el Comité del Espacio Europeo de Datos Sanitarios. Además, ENISA deberá mantener un diálogo constante con el Consejo Consultivo sobre Ciberseguridad Sanitaria para los sectores público y privado sobre la ejecución de las acciones facilitadas por el Centro de Apoyo.

Los informes periódicos de ENISA, como el Informe sobre el estado de la ciberseguridad en la Unión, que ofrece una evaluación agregada del nivel de madurez de las capacidades y recursos de ciberseguridad en toda la UE, incluido el sector sanitario, deberán servir de oportunidad para publicar los datos pertinentes, en apoyo del seguimiento del Plan de Acción. Además, el índice de ciberseguridad de la UE de ENISA[52] puede proporcionar datos cuantitativos y cualitativos que sirvan de base empírica para evaluar el carácter crítico y la madurez del sector sanitario.

8. Siguientes etapas

La presente Comunicación ha establecido un ambicioso programa para reforzar la ciberseguridad del sector sanitario de la UE. Con el desarrollo del Centro de Apoyo a la Ciberseguridad para Hospitales y Prestadores de Asistencia Sanitaria en el seno de ENISA, el Plan de Acción establece una vía hacia la creación de un enfoque europeo común y coherente para hacer frente al reto de la ciberseguridad en el sector.

---

[50] Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32013L0040

[51] El Convenio sobre la Ciberdelincuencia (Convenio de Budapest, STCE n.º 185) y sus Protocolos: https://www.coe.int/en/web/cybercrime/the-budapest-convention

[52] ENISA, índice de ciberseguridad de la UE, marco y nota metodológica (2024). Disponible en https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

Esta Comunicación debe considerarse el inicio de un proceso para mejorar la ciberseguridad en el sector sanitario. Por lo tanto, la adopción del Plan de Acción irá acompañada de la puesta en marcha de amplias consultas con las partes interesadas y de la continuación de los intercambios con los Estados miembros y las redes pertinentes para recabar información. Sobre la base de los resultados de las consultas, la Comisión tiene previsto presentar recomendaciones en el cuarto trimestre de 2025 para perfeccionar el Plan de Acción.

La Comisión pide a los Estados miembros y a todas las partes interesadas que colaboren para cumplir la ambición del Plan de Acción.

ANEXO — Resumen de las acciones propuestas

Comisión:

Centro de Apoyo a la Ciberseguridad de ENISA para hospitales y prestadores de asistencia sanitaria	
Garantizar recursos adecuados para el Centro de Apoyo a la Ciberseguridad Colaborar con el ECCC para poner en marcha proyectos piloto con el fin de desarrollar mejores prácticas de ciberhigiene y evaluación de riesgos en materia de seguridad, y para abordar la necesidad de un seguimiento continuo de la ciberseguridad, la inteligencia frente a amenazas y la respuesta a incidentes utilizando soluciones de ciberseguridad de vanguardia, para el desarrollo del conjunto de servicios del Centro Europeo de Apoyo a la Ciberseguridad	2025
Prevención de incidentes de ciberseguridad	
En consulta con el Grupo de Cooperación SRI, la EU-CyCLONe y ENISA, estudiar la posibilidad de determinar la salud como un sector al que se puede apoyar para la realización de pruebas coordinadas de preparación en el marco de la Ley de Cibersolidaridad	Primer trimestre de 2025
Respuesta rápida y recuperación	
Garantizar, junto con ENISA, que la Reserva de Ciberseguridad de la UE incluya un servicio de respuesta rápida específico para el sector sanitario	Cuarto trimestre de 2025
Cooperación entre los sectores público y privado	
Con el apoyo de ENISA, crear un Consejo Consultivo sobre Ciberseguridad Sanitaria conjunto	Primer trimestre de 2025
Lanzar un llamamiento a la acción para que las empresas de ciberseguridad, las fundaciones, las instituciones educativas y las partes interesadas del sector se comprometan a emprender acciones para abordar los retos de este	Segundo trimestre de 2025
Disuasión de los agentes de riesgo	
Estudiar, junto con la alta representante, el uso del conjunto de instrumentos de ciberdiplomacia para prevenir, desincentivar, y dar respuesta a las	2025

actividades malintencionadas contra los sistemas sanitarios	
Avanzar en la cooperación internacional contra los agentes implicados en programas de secuestro de archivos, en particular en la Iniciativa Internacional contra los Programas de Secuestro de Archivos, en colaboración con la alta representante	2025-2026
Buscar la cooperación en el Grupo de Trabajo sobre Ciberseguridad del G7 para reforzar la ciberseguridad del sector sanitario	2025-2026
Siguientes etapas	
Poner en marcha consultas exhaustivas con las partes interesadas	Primer trimestre de 2025
Aprobar recomendaciones para seguir perfeccionando el Plan de Acción	Cuarto trimestre de 2025

ENISA:

Centro Europeo de Apoyo a la Ciberseguridad para hospitales y prestadores de asistencia sanitaria	
Iniciar la labor de establecer un Centro Europeo de Apoyo a la Ciberseguridad para hospitales y prestadores de asistencia sanitaria	Segundo trimestre de 2025
Desarrollar un amplio catálogo de servicios que proporcionará el Centro de Apoyo a la Ciberseguridad	A partir del cuarto trimestre de 2025
Prevención de incidentes de ciberseguridad	
Publicar orientaciones que destaquen las prácticas de ciberseguridad más críticas y ayuden a los prestadores de asistencia sanitaria a aplicarlas	Tercer trimestre de 2025
En estrecha colaboración con la Comisión y los Estados miembros, desarrollar una herramienta de cartografía normativa	Primer trimestre de 2025
Desarrollar un marco para las evaluaciones de madurez de la ciberseguridad específicas de la asistencia sanitaria	Tercer trimestre de 2025
Llevar a cabo una evaluación anual de la madurez cibernética en el ámbito de la salud	2025-2026

Colaborar con los Estados miembros y las autoridades regionales encargadas de los programas para crear programas modelo de bonos de ciberseguridad	2025-2026
Desarrollar nuevas directrices de contratación pública para la ciberseguridad de los hospitales y los prestadores de asistencia sanitaria	Tercer trimestre de 2025
Crear una red europea de responsables centrales de seguridad informática en el ámbito de la salud	Primer trimestre de 2026
Diseñar y promover módulos de formación y cursos para profesionales sanitarios	Primer trimestre de 2026
Capacidades europeas para la detección de ciberamenazas contra el sector sanitario	
Crear un catálogo europeo de vulnerabilidades aprovechadas conocidas para productos sanitarios, sistemas de historiales médicos digitales y proveedores de equipos y programas informáticos en el ámbito de la salud	Cuarto trimestre de 2025
Introducir un servicio de suscripción de alerta temprana a escala de la UE para el sector sanitario	A partir de 2026
Apoyar al ISAC sanitario europeo con herramientas e intercambio de información	2025-2026
Respuesta rápida y recuperación	
Garantizar, junto con la Comisión, que la Reserva de Ciberseguridad de la UE incluya un servicio de respuesta rápida específico para el sector sanitario	Cuarto trimestre de 2025
En colaboración con la red de CSIRT, desarrollar manuales de respuesta a incidentes cibernéticos adaptados a la asistencia sanitaria.	Tercer trimestre de 2025
Facilitar un amplio despliegue de ejercicios nacionales de ciberseguridad para probar los manuales de actuación y reforzar los protocolos de respuesta a incidentes	A partir del cuarto trimestre de 2025
Proporcionar un servicio de suscripción para la recuperación de datos tras el secuestro de archivos	A partir de 2026
Junto con Europol, identificar las cepas de programas de secuestro más comunes dirigidas a las organizaciones sanitarias y ampliar el repositorio de	Cuarto trimestre de 2025

herramientas de descifrado a través del proyecto «No More Ransom»	
Junto con Europol, desarrollar orientaciones accesibles para ayudar a los prestadores de asistencia sanitaria a evitar el pago de rescates	Tercer trimestre de 2025
Medidas nacionales	
Ayudar a los Estados miembros a elaborar planes de acción nacionales	2025
Coordinar los esfuerzos para garantizar que los recursos y las estrategias de los distintos Estados miembros se complementen entre sí	2025-2026
Aplicación y seguimiento del Plan de Acción	
En consulta con la Comisión, proporcionar actualizaciones periódicas sobre el trabajo del Centro de Apoyo a la Ciberseguridad a las redes pertinentes de los Estados miembros	2025-2026
Intercambio continuo de información con el Consejo Consultivo sobre Ciberseguridad Sanitaria	2025-2026

Estados miembros:

Capacidades europeas para la detección de ciberamenazas contra el sector sanitario	
Transmitir las notificaciones de incidentes procedentes de hospitales y prestadores de asistencia sanitaria en el marco de la SRI 2 al Centro Europeo de Apoyo a la Ciberseguridad	A partir del cuarto trimestre de 2025
Fomentar el desarrollo de los ISAC sanitarios nacionales	2025-2026
Prevención de incidentes de ciberseguridad	
En el marco del Grupo de Cooperación SRI, llevar a cabo una evaluación coordinada de los riesgos en materia de seguridad, evaluando los riesgos tanto técnicos como estratégicos relacionados con las cadenas de suministro de productos sanitarios	Cuarto trimestre de 2025

Respuesta rápida y recuperación	
Facilitar un amplio despliegue de ejercicios nacionales de ciberseguridad para probar los manuales de actuación y reforzar los protocolos de respuesta a incidentes	A partir de 2026
Medidas nacionales	
Designar Centros Europeos de Apoyo a la Ciberseguridad para hospitales y prestadores de asistencia sanitaria	Segundo trimestre de 2025
Crear planes de acción nacionales centrados en la ciberseguridad en el sector sanitario	Cuarto trimestre de 2025
Facilitar la puesta en común de recursos entre los prestadores de asistencia sanitaria	2025-2026
Establecer parámetros de referencia no vinculantes y supervisar los objetivos de financiación destinados específicamente a la ciberseguridad	Cuarto trimestre de 2025
Solicitar a las organizaciones sanitarias y otras entidades sujetas a la Directiva SRI 2 que informen de sus intenciones de pagar rescates	Cuarto trimestre de 2025