Recomendaciones de la Agencia Europea de Ciberseguridad ante incidentes de seguridad en el sector sanitario

Magdalena Jareño Butron
Técnica Superior Informática

José Antonio Arratibel Arrondo
(Interventor en el Servicio Vasco de Salud-OSAKIDETZA)
Gobierno Vasco-Eusko Jaurlaritza

Revista Auditoría Pública nº 83
junio 2024. Páginas: 115-137

Resumen: En este trabajo pretendemos hacer una reflexión, partiendo del marco jurídico relativo a la articulación de los sistemas de respuesta a incidentes informáticos de los países de la Unión Europea frente a los ciberataques en el ámbito sanitario y hospitalario y, en última instancia, a los datos personales de salud que gozan de una especial protección jurídica. La nueva normativa europea de protección de datos (RGPD), considera esta información como especialmente protegida por las administraciones gubernamentales. A modo de ejemplo, recordamos el último ciberataque que sufrió un centro sanitario del Estado, el Hospital Clínic Barcelona el pasado 5 de marzo, y el esfuerzo de la Agencia de Ciberseguridad de Catalunya para el análisis y recuperación de los sistemas de información robados. En este sentido, la Agencia de la Unión Europea para la Ciberseguridad es la organización que coordina la ciberseguridad del sector sanitario en el espacio europeo. Ha elaborado una serie de protocolos que, en un futuro cercano, serán parte de la regulación positiva del sector. Además de la experiencia de los países del entorno europeo, destacamos que se está desarrollando un movimiento organizado a nivel mundial para crear y coordinar equipos de respuesta a ciberataques al sector sanitario con el fin de proteger los datos de salud de los pacientes. En definitiva, un trabajo necesariamente interdisciplinar que requiere tener en cuenta el derecho positivo de la protección de los datos personales de salud y, el técnico de la ingeniería informática actual, para garantizar dichos derechos de la forma más segura posible.

Palabras Clave: ENISA, RGPD, protección de datos personales salud, ciberseguridad hospitalaria.

Abstract: In this work we intend to reflect, starting from the legal framework related to the articulation of the response systems to computer incidents of the countries of the European Union against cyber attacks in the health and hospital field and, ultimately, to the data health personnel who enjoy special legal protection. The new European data protection regulations (GDPR) consider this information to be especially protected by government administrations. As an example, we remember the last cyber attack suffered by a State health center, the Hospital Clínic Barcelona, on March 5, and the efforts of the Cybersecurity Agency of Catalonia to analyze and recover stolen information systems. In this sense, the European Union Agency for Cybersecurity is the organization that coordinates cybersecurity in the health sector in the European space. It has developed a series of protocols that, in the near future, will be part of the positive regulation of the sector. In addition to the experience of the countries in the European environment, we highlight that an organized movement is developing worldwide to create and coordinate response teams to cyber attacks on the health sector in order to protect patients' health data. In short, a necessarily interdisciplinary work that requires taking into account the positive right to the protection of personal health data and the current computer engineering technician, to guarantee these rights in the safest way possible.

Keywords: ENISA, GDPR, personal health data protection, hospital cybersecurity.

SUMARIO

I. Introducción.

El volumen y la intensidad de los ataques cibernéticos en el sector de la salud han aumentado a partir de 2020. Las organizaciones sanitarias, en general, y los hospitales, en particular, han sido un objetivo importante para el delito cibernético, principalmente, debido al valor de los datos que se pueden obtener de un ataque, así como su impacto disruptivo. Como infraestructura y servicios críticos que son, las organizaciones de atención de la salud (hospitales, centros sanitarios de atención primaria y especializada etc.), tanto públicas como privadas, deben prepararse para enfrentarse a este tipo de ciberataques. La interrupción de sus servicios esenciales conduciría a un impacto grave tanto en los gobiernos europeos como en sus ciudadanos.

En un mundo marcado por la hiperconectividad la actividad de los ciberdelincuentes plantea una amenaza importante para la seguridad interna de la Unión Europea y para la seguridad en línea de sus ciudadanos. La pandemia de COVID-19 ha puesto en relieve la necesidad de una mayor seguridad en el mundo digital. Las personas han incrementado su presencia en línea, tanto para mantener relaciones personales como profesionales, a la vez que los ciberdelincuentes han sabido sacar provecho de los sistemas de atención sanitaria.

Al mismo tiempo, todo usuario del sistema sanitario tiene derecho a la constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud, sobre sus datos médicos personales. Este

aumento del procesamiento de datos médicos digitalizados también ha aumentado los riesgos, en términos de la ciberseguridad, la protección de datos y la probabilidad de violaciones de datos protegidos. Instrumentos legales pertinentes de la UE, como la Directiva NIS, el Reglamento General de Protección de Datos (RGPD), el Reglamento de Dispositivos Médicos, la Directiva sobre la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, etc. impuso obligaciones a proveedores de atención médica y fabricantes de dispositivos médicos para garantizar una adecuada y uniforme nivel de protección de los datos médicos y los productos y servicios que los utilizan.

En nuestro ordenamiento jurídico la protección de estos datos personales es un derecho fundamental recogido en el artículo 18.4 de la Constitución Española y regulado el RGPD, y la Ley de protección de datos (LOPDGDD). En este caso en particular, la normativa en protección de datos se complementa con la Ley de Autonomía del Paciente 41/2002, de 14 de noviembre. La ley de protección de datos médicos se encarga de regular los derechos y las obligaciones en materia de información y documentación clínica en la que se regula su historial. Esta normativa afecta al personal que operan en el sector sanitario, a las clínicas, a los hospitales, a los centros médicos y a las instituciones sanitarias. Además, el RGPD distingue, en el art. 9, datos relativos a la salud como categoría especial de datos (sensibles) y conjuntos establecer requisitos adicionales y obligaciones más estrictas para el procesamiento y protección de dichos datos, en para salvaguardar los derechos y libertades de las personas (interesados).

Para hacer frente a tales amenazas, los Estados miembros de la UE y las entidades públicas y privadas europeas han iniciado un proceso de reflexión con el objetivo de fortalecer la respuesta a incidentes y ataques cibernéticos en el sector sanitario. En este sentido, el actor fundamental es la Agencia de la Unión Europea para la Ciberseguridad (ENISA). La Agencia Europea trabaja para fortalecer las relaciones públicas y privadas dentro del sector de la salud construyendo un círculo de confianza a escala europea con el fin de una mejor comprensión de los equipos de respuesta a Incidentes de Seguridad Informática, en los que confían en caso de un ciberataque importante y sistémico. Para tal fin, los estudios recomiendan potenciar y crear equipos de respuesta europeos debidamente coordinados, que apoyen a los operadores de servicios esenciales sanitarios de los países miembros de la UE con el fin de desarrollar capacidades de respuesta conjunta a ciberataques.

No cabe duda de que estas conclusiones sentarán la base para la ulterior elaboración de la normativa europea en materia de ciberseguridad sanitaria colmando, de esta manera, los aspectos técnicos y jurídicos del derecho a la privacidad de los datos personales de salud en la Unión Europea.

II. La Agencia de la Unión Europea para la Ciberseguridad.

Las organizaciones sanitarias, en general, y los hospitales, en particular, han sido un objetivo importante para el delito cibernético, principalmente, debido a el valor de los datos que se pueden obtener de un ataque, así como su impacto disruptivo[1]. Para hacer frente a tales amenazas, los Estados miembros y las entidades públicas y privadas europeas han iniciado un proceso de reflexión con el objetivo de fortalecer la respuesta a Incidentes y ataques cibernéticos (en adelante IR), así como la capacidad de respuesta ante los incidentes (en adelante IRC) y la coordinación entre Equipos de respuesta a Incidentes de Seguridad Informática (en adelante CSIRT)[2].

El actor fundamental en el espacio europeo de la ciberseguridad del sector sanitario es la Agencia de la Unión Europea para la Ciberseguridad (ENISA)[3]. La Agencia fue creada en 2004 y reforzada por el Reglamento sobre la Ciberseguridad de la UE y contribuye a la política de seguridad cibernética de la UE, mejora la fiabilidad de los productos, servicios y procesos de Tecnologías de la Información y Comunicación (TIC) mediante programas de certificación de la ciberseguridad, coopera con los Estados miembros y con los organismos de la UE y ayuda a Europa a prepararse para los desafíos del mañana en materia de ciberseguridad. Mediante el intercambio de conocimientos, la creación de capacidades y la sensibilización, la Agencia coopera con las principales partes interesadas para fortalecer la confianza en la economía conectada, impulsar la resiliencia de las infraestructuras de la Unión y, por último, proteger a la sociedad y a la ciudadanía europea de las amenazas digitales.

1 https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-health care-institutions-with-ransomware

2 En su terminología en inglés: Incident Response (IR), Incident Response Capabilities (IRC) and capabilities and Theo coordination betw een Compute Security Incident Response Teams (CSIRT).

3 European Union Agency for Cybersecurity.

La normativa por la que se rige ENISA es el (Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a la ENISA (la Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»). En este sentido, las funciones principales que tiene la Agencia de la Unión Europea para la Ciberseguridad las podemos clasificar en las siguientes:

A. Objetivos.

Los objetivos estratégicos de ENISA se derivan de su reglamento y de aportes de los Estados miembros y las comunidades relevantes, incluido el sector privado. En cooperación y en apoyo de los Estados miembros y las instituciones de la Unión, ENISA busca lograr:

- Experiencia: apoya a Europa para enfrentar los desafíos emergentes de seguridad de la red y de la información, mediante la recopilación, el análisis y la puesta a disposición de información y experiencia sobre cuestiones clave de NIS que puedan afectar a la UE, teniendo en cuenta la evolución del entorno digital.

- Política: promueve la seguridad de las redes y la información como una prioridad política de la UE, ayudando a las instituciones de la Unión Europea y a los Estados miembros a desarrollar e implementar políticas y leyes de la UE relacionadas con los NIS.

- Capacidad de soporte: mantiene el estado de la red y las capacidades de seguridad de la información, ayudando a los Estados miembros y los organismos de la Unión Europea a reforzar sus capacidades NIS.

- Fomentar la emergente comunidad europea de seguridad de redes e información, reforzando la cooperación a nivel de la UE entre los Estados miembros, los organismos de la Unión Europea y las partes interesadas, incluido el sector privado.

B. Funciones.

Un aspecto importante después de establecer un CSIRT es definir sus servicios principales de acuerdo con los recursos internos disponibles. Los servicios centrales de CSIRT se pueden agrupar en tres categorías principales:

- Los servicios reactivos generalmente consisten en informes posteriores a incidentes del sector afectado u otros episodios relacionados con amenazas o ataques, como servidores comprometidos, malware, vulnerabilidades u otro tipo de incidentes similares (alertas y advertencias, respuesta a incidentes, manejo de vulnerabilidad y manejo de equipos).

- Los servicios proactivos están diseñados para detectar y prevenir ataques antes de que haya un impacto real en los sistemas de producción. En esta categoría de servicios, la información generada por los equipos CSIRT se difunde a su sector correspondiente para evitar ser blanco de un ataque.

- Servicios de gestión de la seguridad para revisar y mejorar la posición de seguridad de las organizaciones de un sector. (análisis de riesgo, planificación de BC y DR, conciencia de seguridad y formación).

C. Gestión de crisis cibernéticas.

ENISA trabaja con la UE, los Estados miembros, la Comisión Europea y otras agencias para ayudar a prevenir o responder de manera efectiva a los incidentes y crisis de seguridad cibernética. Ha estado apoyando el campo de la gestión de crisis e incidentes cibernéticos europeos durante varios años, con actividades como: simulaciones de crisis, entrenamientos, apoyo a los Estados miembros para desarrollar sus planes y estructuras de crisis, conferencias internacionales y estudios en ciberseguridad.
Por tanto, la Agencia de la Unión Europea para la Ciberseguridad se ha convertido en el referente de la gestión de crisis cibernéticas a nivel de la UE. Trabaja en estrecha colaboración con los Estados miembros para desarrollar procedimientos de gestión de crisis cibernéticas, a nivel de la UE, para mejorar el conocimiento de una situación concreta de crisis en caso de incidentes cibernéticos transfronterizos, para ayudar tanto a nivel nacional como a nivel de la UE a adoptar las medidas correctoras más oportunas. También ejecuta simulaciones y ejercicios de crisis y ofrece entrenamientos sobre este tema.

D. Ejercicios cibernéticos.

Una gran parte de los esfuerzos de la Agencia para el desarrollo capacidades de prevención se centran en los ejercicios cibernéticos. Las siguientes son algunas de las actividades de ejercicio cibernético: programa de ciber Europa, plataforma de ejercicio cibernético (CEP), entrenamientos y estudios.

E. Educación en ciberseguridad.

Las actividades en el área de educación y conciencia general buscan promover las habilidades NIS y apoyar a la Comisión para mejorar las habilidades y la competencia de los profesionales en esta área. Dentro de esta función se encuentra el European Cyber Security Challenge[4]. Los concursantes resuelven desafíos relacionados con la seguridad de dominios como: seguridad web y de red seguridad móvil, cripto rompecabezas, ingeniería inversa y forense digital.

F. Protección de datos.

En el mundo actual de servicios digitales, redes sociales e Internet de las cosas, estamos experimentando una recopilación a gran escala sin precedentes y un mayor procesamiento de datos personales. Esta nueva sociedad basada en datos pres extendidas de vigilancia electrónica, creación de perfiles y divulgación de información privada.

G. Informe de incidentes.

Un instrumento importante de la legislación de ciberseguridad de la UE son los informes de incumplimiento de ciberseguridad. La notificación de violaciones de seguridad cibernética es importante no solo para los ciudadanos sino también para ayudar a las autoridades nacionales con sus tareas de supervisión. En la UE existen varias leyes diferentes sobre denuncias de incumplimiento. En 2018 entró en vigor la Directiva de la UE sobre seguridad de redes y sistemas de información (llamada Directiva NIS), que introdujo reglas de notificación de incidentes de ciberseguridad para operadores de servicios esenciales en una amplia gama de sectores críticos, como la energía, el transporte, finanzas y salud. Recientemente, el 27 de diciembre de 2022 se publicó la Directiva (UE) 2022/2555, del Parlamento Europeo y del Consejo, de 14 de, diciembre de 2022, conocida como NIS 2, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión. Esta Directiva establece obligaciones de ciberseguridad para los Estados miembros, medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades en su ámbito de aplicación, obligaciones relativas al intercambio de

4 Se trata del mayor campeonato técnico a nivel europeo en materia de ciberseguridad, en el que compiten los mejores jóvenes talentos de los diferentes países participantes, seleccionados a través de sus diferentes competiciones nacionales. Los concursantes resuelven desafíos relacionados con la seguridad de dominios como: seguridad web y de red seguridad móvil, cripto rompecabezas, ingeniería inversa y forense digital. Así, INCIBE organiza anualmente una competición específica para la confeccionar el equipo nacional. En 2016 y 2017, la selección española fue la vencedora de esta competición, convirtiéndose en referencia en materia de ciberseguridad. Asimismo, la edición de 2017 que tuvo lugar en Málaga (España), fue organizada por INCIBE y contó con una gran participación de selecciones nacionales.

información sobre ciberseguridad, así como obligaciones de supervisión y ejecución para los Estados miembros[5]. La transposición de la directiva ha de efectuarse, a más tardar el 17-10-24 los Estados miembros deberán adoptar y publicar las medidas necesarias para dar cumplimiento a lo establecido en la Directiva.

Nos parece especialmente importante que esta directiva NIS 2 amplía su ámbito de aplicación para abarcar a entidades medianas y grandes de más sectores críticos para la economía y la sociedad, incluyendo proveedores de servicios públicos de comunicaciones electrónicas, servicios digitales, gestión de aguas residuales y residuos, fabricación de productos críticos, servicios postales y de mensajería, así como a las Administraciones Públicas. En el caso de España afecta a las Entidades de la Administración General del Estado, Entidades de las Administraciones Públicas de Comunidades Autónomas y se podrá determinar su aplicación a entidades de la Administración Pública a nivel local.

Para hacer frente a tales amenazas, los Estados miembros y las entidades públicas y privadas europeas han iniciado un proceso de reflexión, liderado por la Agencia de la UE, con el objetivo de fortalecer la respuesta a Incidentes y ataques cibernéticos (en adelante IR), así como la capacidad de respuesta ante los incidentes (en adelante IRC) y la coordinación entre Equipos de respuesta a Incidentes de Seguridad Informática (en adelante CSIRT) en el sector sanitario.

III. Marco jurídico europeo y respuesta a incidentes de Seguridad Informática en el sector sanitario.

La Agencia de la Unión Europea para la Ciberseguridad ha elaborado distintos informes que tienen como objetivo apoyar la comprensión del estado actual y desarrollo de los equipos CSIRT sanitarios en la UE[6]. Sus conclusiones pretenden ayudar a los miembros Estados para identificar problemas y mejorar la respuesta al manejo de incidentes (IR) dentro del sector de la salud, tras la transposición a los Estados miembros de la Directiva NIS[7].

Los estudios analizan las posibles brechas, superposiciones y desafíos en los servicios ofrecidos, así como como en los procedimientos, procesos y herramientas implantadas. Más específicamente, el estudio proporciona una descripción general de los factores clave que facilitan o dificultan el desarrollo de los equipos CSIRT sectoriales sanitarios, así como la descripción de los recursos y herramientas específicos para apoyar el desarrollo de las capacidades de respuesta a incidentes y ataques cibernéticos (IRC) en el sector de la salud.

Los principales objetivos de los informes a que hemos hecho referencia son los siguientes: recopilar datos sobre el IRC actual en el sector sanitario; analizar esa información para evaluar las capacidades sectoriales de la atención de la saludad actuales (servicios, procesos, herramientas y mecanismos de cooperación); extraer conclusiones y recomendaciones en base a los aspectos clave que faciliten y/o entorpecer los procedimientos de respuesta IR.

Lo más interesante, a nuestro juicio, de estos estudios ha sido: en primer lugar, recopilar información del marco jurídico relevante para proporcionar estadísticas de distribución de servicios ofrecidos al sector sanitario por equipos CSIRT y otras respuesta a incidente de seguridad IR; en segundo lugar, el análisis de brechas y superposiciones en servicios, procesos, herramientas, recursos, especialmente entre los CSIRT y otras entidades IR dentro del sector salud; y, por último, conclusiones y recomendaciones para el desarrollo de equipos CSIRT y otras entidades IR.

La Agencia de la Unión Europea para la Ciberseguridad diseñó un cuestionario distribuido a los CSIRT nacionales de la UE y CSIRT sectoriales sanitarios para identificar, recopilar y analizando datos sobre el desarrollo y las capacidades de IR en el sector de la atención de la salud[8].

5 Se modifican el Reglamento (UE) ni 910/2014 y la Directiva (UE) 2018/1972 y se deroga la Directiva (UE) 2016/1148

6 Los informes que hemos analizado para la elaboración del presente trabajo han sido: ENISA: CSIRT Capabilities in Halthcare Sector (november 2021). ENISA: Cloud Security foro Healthcare Services (2021). ENISA: CSIRT Capabilities in Halthcare Sector (november 2021). ENISA: Procurement Guidelines for Cybersecurity in Hospitals (2020). ENISA: Pseudonymisation techniques and best practices. (2019). ENISA: Procurement Guidelines for Cybersecurity in Hospitals. (2020). ENISA, CSIRT Capacidades. ¿Cómo evaluar la madurez? Directrices para los organismos nacionales y gubernamentales (2019).

7 El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, incorpora al ordenamiento jurídico español la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, más conocida como Directiva NIS, que busca identificar los sectores en los que se debe garantizar la protección de las redes y sistemas de información y establecer las exigencias de notificación de ciberincidentes. La Directiva (UE) 2016/1148 quedará derogada con efectos a partir del 18 de octubre de 2024.

8 Recogido en el informe de ENISA: CSIRT Capabilities in Halthcare Sector (november 2021).

El alcance de la investigación y el enfoque para la recopilación de datos se centró en el aspecto operativo, y definió el método de recopilación de datos siguiente:

1. Revisión de la literatura sobre el sector salud IR. La finalidad ha sido analizar todos los aspectos de las responsabilidades de los IR dentro del sector de la salud para facilitar información a los CSIRT y otras entidades en cada Estado miembro de la UE. Este análisis consistió en identificar los organismos y/u organizaciones relevantes que juegan un papel en el campo de la capacidad de respuesta a incidentes cibernéticos dentro del sector de la salud en la Unión Europea; y analizar las responsabilidades de IR de las diferentes partes interesadas, centrándose en los aspectos operativos de la respuesta a incidentes informáticos[9].

2. Encuesta en línea. Sobre el diseño de un cuestionario la Agencia ha recopilado datos relevantes sobre los principales factores que facilitan y obstaculizan el establecimiento de equipos CSIRT sectoriales, así como los recursos y herramientas disponibles para apoyar el desarrollo de capacidades de respuesta a incidentes (IRC) en el sector salud.

3. Realización de la encuesta. Tras la validación, el cuestionario se distribuyó a los distintos órganos competentes de los países europeos. La encuesta incluyó una introducción a los objetivos del estudio, instrucciones sobre cómo responder al cuestionario y una declaración de privacidad. La encuesta estuvo disponible en línea durante cuatro semanas. Un total de 15 proporcionaron respuestas en representación de 12 Estados miembros.

4. Análisis e identificación de recomendaciones. Este análisis preliminar permitió al equipo de trabajo el mapeo de los hallazgos clave del estudio.

5. Informe final. Observaciones finales y/o comentarios del grupo de expertos que se utilizaron para validar el estudio.

9 Esto consistió fundamentalmente en revisamos publicaciones anteriores de ENISA, políticas documentos, estrategias nacionales y otros documentos e informes puestos a disposición por los CSIRT, Centros Nacionales de Ciberseguridad, y la Comisión Europea. También se han consultado los estudios tecnológicos de empresas de investigación estratégica e investigadores académicos, así como consultas informales con expertos en relaciones internacionales.

III.1. Análisis comparativo.

Un análisis de la normativa de los países miembro de la UE proporciona los datos actuales básicos del diseño y la configuración de respuesta a incidentes IR sectorial, a nivel europeo. En base a los informes de la Agencia citados hemos efectuado un análisis comparativo de la situación jurídica relativa los países miembros de la UE, atendiendo a la regulación de equipos de respuesta a emergencias informáticas, específicamente para instituciones del sector sanitario[10]. El resultado ha sido la clasificamos en cuatro grupos, a saber:

A. No hay equipos de respuesta específicos para el sector sanitario.

La gran mayoría de los Estados miembros (20 de los 27) no han creado equipos de Respuesta a Emergencias Informáticas en el sector sanitario: Alemania, Bélgica, Chipre, Republica checa, Estonia, Finlandia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Malta, Polonia, Portugal, Rumania, Eslovaquia, Eslovenia, España y Suecia. Los servicios de respuesta a incidentes son prestados por el CSIRT nacional/gubernamental de cada Estado para todos los sectores, incluido el sanitario. Esto se aplica en particular a los países con un modelo centralizado de respuesta a incidentes, que no tienen previsto desarrollar capacidades sectoriales específicas.

- **Bélgica:** el CERT.be, es el servicio operativo del Centro para la Seguridad Cibernética de Bélgica (CCB) que actúa en el caso de ataques significativos en línea contra la infraestructura sanitaria belga. No tiene un CSIRT dedicado entidad para el sector salud.

- **Alemania:** el CERT-Bund (Computer Emergency Response para Agencias Federales) es el punto central de contacto para medidas preventivas y reactivas relativas a incidentes informáticos relacionados con la seguridad. En Alemania no existe una entidad especializada en el sector sanitario.

- **Chipre:** el CSIRT-CY es el servicio operativo de la Seguridad Informática Nacional y equipo de respuesta a incidentes. No existe una entidad dedicada al sector salud.

- **Republica Checa:** el CSIRT.CZ es el CSIRT Nacional de la República Checa que actúa en el caso de ataques significativos en línea contra la infraestructura sanitaria. No tiene un CSIRT Sectorial de Salud.

- **Estonia:** el CERT-EE es la organización responsable de la gestión de incidentes de seguridad que actúa en el caso de ataques significativos en línea contra la infraestructura sanitaria. No tiene un CSIRT Sectorial de Salud.

- **Finlandia:** el Centro Nacional de Seguridad Cibernética de Finlandia (NCSCFI) es responsable de la supervisión de todos CSIRT. Tiene una eficiente autoridad supervisora del sector salud. No hay planes concretos par aun sector CSIRT específico sanitario.

- **Grecia:** el GR-CSIRT es el equipo cibernético de defensa, respuesta a incidentes y Operaciones. Es la organización responsable de la gestión de incidentes de seguridad que actúa en el caso de ataques significativos en línea contra la infraestructura sanitaria. No tiene un CSIRT Sectorial de Salud.

- **Hungría:** existen tres unidades organizativas en la Seguridad Cibernética Nacional. La unidad Gov CERT Hungary es responsable de la gestión de incidentes de seguridad en el caso de ataques significativos en línea contra la infraestructura sanitaria. No tiene un CSIRT Sectorial de Salud.

- **Irlanda:** el CSIRT-IE es el organismo dentro de la Cibernética Nacional Security Center (NCSC) asiste a los incidentes de seguridad cibernética a nivel nacional. El CSIRT-IE también actúa como un punto de contacto nacional para ataques cibernéticos que involucran entidades de atención médica dentro de Irlanda. No hay entidad dedicada al sector salud.

- **Italia:** el Equipo de Respuesta a Incidentes de Seguridad Informática se encuentra dentro del Departamento de Seguridad. No existe una entidad dedicada al sector salud.

- **Letonia:** el CERT.LV es la Institución de Seguridad de las Tecnologías de la Información de la República de Letonia. Su misión es promover la seguridad de las tecnologías de la información (TI) en Letonia. Letonia no dispone de una entidad dedicada al sector salud.

10 Ver Anexo donde recogemos una tabla resumen de la situación jurídica de los países miembros de la UE en materia de respuestas a incidentes informáticos en el sector sanitario.

- **Lituania:** el CERT-LT40 es el servicio nacional de gestión de incidentes de seguridad de las redes de comunicaciones electrónicas y de la información que opera como Equipo de Respuesta a Emergencias Informáticas. En Lituania no existe entidad dedicada al sector sanitario en Lituania.

- **Malta:** el CSIRT Malta es el servicio nacional de gestión de incidentes de seguridad a las infraestructuras críticas de Malta. En Malta no existe una entidad dedicada al sector salud.

- **Polonia:** los tres CSIRT nacionales son el Computer Security Incident Response Team (CSIRT GOV), el Equipo de Respuesta a Incidentes de Seguridad Seguridad Informática del Ministerio de Defensa polaco (CSIRT MON) y el de Respuesta a Emergencias Informáticas CERT-POLSKA, que contribuyen a garantizar la ciberseguridad a nivel ciberseguridad a nivel nacional. No existe una entidad dedicada al sector de la salud.

- **Portugal:** el CERT.PT es un servicio integrado en su Centro Nacional de Ciberseguridad que coordina la respuesta a incidentes relacionados con el ciberespacio nacional. No cuenta con un CSIRT Sectorial de Salud.

- **Rumania:** el CERT.RO48 es el Equipo Nacional de Respuesta a Emergencias Informáticas de Rumanía. creado como estructura independiente de investigación, desarrollo y peritaje en el ámbito de la ciberseguridad. En Rumanía no existe ninguna entidad dedicada al sector sanitario.

- **Eslovaquia:** el Centro Nacional de Ciberseguridad SK-CERT realiza actividades nacionales y estratégicas en el ámbito Ciberseguridad. No existe una entidad dedicada al sector sanitario.

- **Eslovenia:** el SI-CERT50 (Slovenian Computer Emergency Response Team) es un equipo nacional designado de respuesta a incidentes de seguridad informática que opera en el marco del instituto público Academia e Investigación de Eslovenia. Eslovenia no cuenta con una entidad dedicada al sector sanitario.

- **España:** el INCIBE-CERT es el centro de respuesta a incidentes de seguridad de seguridad de referencia para ciudadanos y entidades operado por el Instituto Nacional Ciberseguridad (INCIBE), dependiente del Ministerio de Economía y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. No existe una entidad dedicada el sector sanitario.

- **Suecia:** el CERT-SE es el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) nacional de Suecia. Apoya a la sociedad en la labor de gestión y prevención de incidentes informáticos. Suecia no dispone de un CSIRT específico para el sector sanitario.

B. Previsto el desarrollo de equipo sectorial sanitario.

Austria y Croacia tienen proyectos normativos para para crear, en un futuro cercano, un equipo sectorial sanitario de respuesta a Emergencias Informáticas.

- **Austria:** el CERT.at es el CERT nacional austriaco. El CERT.at es el principal punto de contacto para la seguridad informática en el contexto nacional. En caso de ataques en línea significativos contra la infraestructura sanitaria austriaca, CERT.at coordinará la respuesta de los operadores afectados y los equipos de seguridad locales. No dispone de un CSIRT sectorial dedicado a la sanidad, pero está trabajando en su planificación.

- **Croacia:** el CERT nacional (CERT.hr) es responsable de prevención de ciberamenazas y protección de la seguridad de los sistemas de información públicos en la República de Croacia. Croacia no dispone de un CSIRT sectorial dedicado a la sanidad, pero está trabajando en su planificación.

C. En preparación un equipo sectorial de salud.

Se encuentran en preparación de un equipo sectorial sanitario de respuesta a Emergencias Informáticas: Bulgaria y Dinamarca. Se están creando actualmente un CSIRT de salud a nivel nacional.

- **Bulgaria:** el CERT Bulgaria) es el Equipo Nacional de Respuesta a Incidentes de Seguridad Informática. Bulgaria está creando CSIRT sectoriales para facilitar la aplicación de la Directiva NIS. Sin embargo, aún no dispone de un CSIRT sectorial de salud.

- **Dinamarca:** El Centro de Ciberseguridad (CFCS)26 es la autoridad nacional de seguridad informática. En Dinamarca, existe un CSIRT del sector sanitario, la Autoridad Danesa de Datos que se encuentra actualmente en fase de desarrollo.

D. Cuentan con equipo sectorial de salud a nivel nacional.

Francia, Países Bajos y Luxemburgo han desarrollados normativamente sus equipos de Respuesta a Emergencias Informáticas, específicamente para instituciones del sector sanitario.

En el caso de Francia: fue creado en el seno de la Agence Nationale de la Sécurité de Sistemas de información (ANSSI), el CERT-FR. Se encarga de poner en marcha los medios para responder a los incidentes o ataques informáticos en Francia. Dispone de un CSIRT sectorial dedicado al sector sanitario, CERT Santé (antes denominado Accompagnement Cyber sécurité des Structures de Santé), que funciona desde 2017.

En el caso de Luxemburgo: existen dos CSIRT nacionales: el Centro de Respuesta a Incidentes Informáticos de Luxemburgo (CIRCL) y GOVCERT, que proporcionan un servicio de respuesta sistemática a las amenazas e incidentes sanitarias. HealthNet-CSIRT (HealthNet Computer Security Incident Response Team) es el punto de contacto para tratamiento de los incidentes informáticos de las distintas partes interesadas activas en el ámbito sanitario.

Por último, en el caso del Sector de Salud de los Países Bajos: ha desarrollado un equipo CSIRT específicamente para instituciones del sector salud. El Centro Nacional de Ciberseguridad (NCSC.NL) es responsable de la coordinación de las medidas de respuesta a incidentes para las instituciones, así como de las entidades relacionadas con infraestructuras críticas. Los Países Bajos cuentan con un CSIRT (Z-CERT) que es un Equipo de Respuesta ante Emergencias Informáticas (CERT) desarrollado específicamente para instituciones del sector sanitario. La principal entidad a cargo de la respuesta a incidentes en el sector salud son los CSIRT Nacionales. Los equipos CSIRT del sector de la salud siguen siendo una excepción en los Estados miembros[11]. Sin embargo, hay una tendencia en el desarrollo de colaboraciones de CSIRT en todo el sector, que incluyen, entre otros, el intercambio de información, experiencia y respuestas ante ataques informáticos[12].

11 https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report

12 https://op.europa.eu/en/publication-detail/-/publication/3b6ad641-d23c-11eb-ac72-01aa75ed71a1

III.2. Cuestiones para tener en cuenta en la futura legislación europea.

La gran mayoría de los miembros de la UE consultado (73%) destacaron la necesidad de apoyo de grupos/foros para el intercambio de información, buenas prácticas y experiencia en respuesta a incidentes de ciberseguridad en el sector de salud. Este intercambio de información es clave para la mejora de la creación de capacidad sectorial de respuestas conjuntas europeas a incidentes informáticos en salud. En este sentido, sugirieron que la necesidad de una estrecha vinculación con las instituciones públicas de la UE, organismos y agencias de la UE para compartir información. Otros foros mencionados son los grupos internacionales, como los miembros de la red de CSIRT.

En la misma línea, los encuestados entienden que las iniciativas existentes de creación de capacidades a nivel europeo, en relación con las herramientas de intercambio de información y las acciones de concienciación, relativos a incidentes de seguridad son muy útiles para mejorar la eficiencia de los equipos de intervención CSIRT sanitarios, frente ataques informáticos, en particular sus capacidades de IR.

Además, se pone de relieve la necesidad de una mayor intervención sobre el uso de sistemas sanitarios de proveedores.

Con respecto a las herramientas/procesos específicos existentes en su organización que ayudarían a mejorar la efectividad de las capacidades de IR del sector en otros CSIRT de Salud, los encuestados señalaron las siguientes necesidades principales:

- Capacitaciones y ejercicios sobre políticas y procedimientos.
- Herramientas de respuesta a vulnerabilidades.
- Acciones de intercambio de información.

Finalmente, hay un consenso generalizado hacia la creación de programas de asociación público-privada, que ayudaría a crear una visión común entre los Operadores de Servicios Esenciales y los equipos de respuesta a incidentes de seguridad informática, minimizando la falta de confianza entre ellos.

Dicho esto, seguidamente vamos a analizar, con mayor detalle, las conclusiones más importantes relativas a la situación en que se encuentran las administraciones sanitarias de la UE en relación a las capacidades de los equipos de respuesta frente a incidentes de ciberseguridad informática en el sector sanitario. Estas conclusiones han de coadyuvar a la normativa comunitaria, en materia de ciberseguridad, que se legisle en un futuro próximo.

III.2.1. Creación de equipos de respuesta.

La primera conclusión que obtenemos de los informes de la Agencia es la necesidad de creación de capacidades de respuesta a incidentes (IR) específicas en el sector de la salud en los países miembros. Las razones fundamentales las podemos agrupar: en primer lugar, la falta de conocimiento sectorial del CSIRT Nacional, en segundo lugar, la importante experiencia acumulada de respuestas a incidentes pasados; y, por último, la implementación de la Directiva NIS en el ámbito europeo.

- La primera razón se centra en la necesidad de superar la falta de conocimiento o capacidad específica del sector sanitario del CSIRT Nacional. Es la razón más relevante que provoca la creación de capacidades IR específicas del sector de la salud (27% de las respuestas).

- La segunda razón más importante (18% de las respuestas) es la puesta en marcha de la Directiva NIS. La legislación europea tiene un impacto importante y positivo en impulsar en los países de la UE el desarrollo de capacidades sectoriales. En particular, los encuestados indicaron que la Directiva NIS tuvo los siguientes impactos sobre su actividad relacionada con la creación de capacidades sectoriales de salud (IR):

- Proporcionó apoyo financiero adicional para medidas de seguridad.
- Cambió las estructuras y arquitecturas de las medidas de ciberseguridad existentes.
- Amplió el alcance de las responsabilidades de los CSIRT.

La ampliación del alcance de las responsabilidades de los CSIRT, combinada con la provisión de apoyo financiero adicional para nuevas medidas de seguridad, parecen haber alentado la creación de capacidades IR específicas del sector.

- Por último, las dificultades en la gestión de los incidentes de ciberseguridad en Sectores de la Directiva NIS (14 % de las respuestas), junto con las experiencias incidentes anteriores (14% de las respuestas), destacó la necesidad de capacidades IR específicas del sector en el sector salud.

  Del estudio de la Agencia destacamos que, además de estas principales razones que llevan a la creación de CSIRT sectoriales y/o capacidades de respuesta a incidentes, existen también otros factores que facilitan su desarrollo. Estos factores facilitadores son, principalmente, los siguientes:

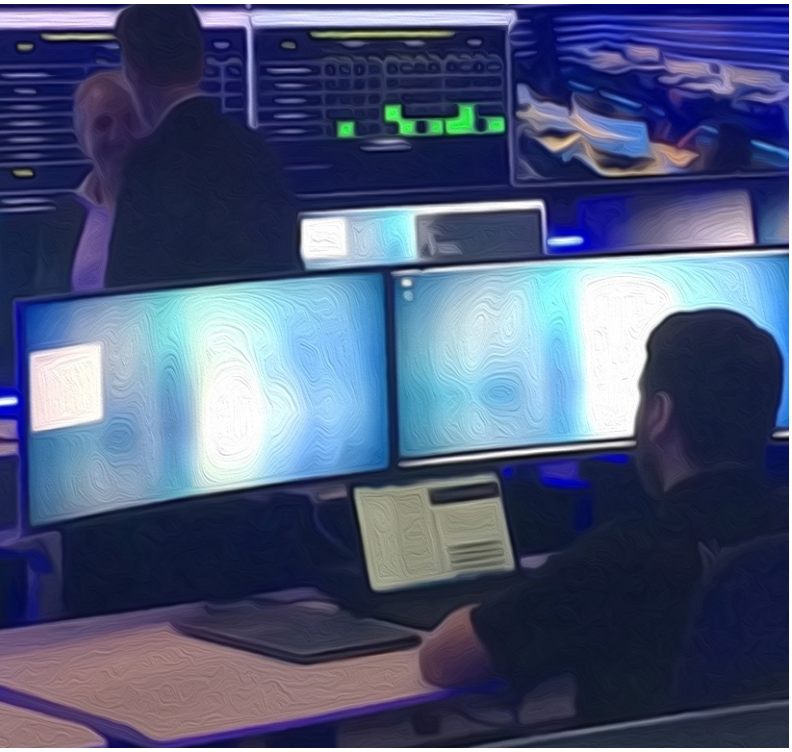
- La difusión del conocimiento de las amenazas, el intercambio de buenas prácticas e información y experiencias compartidas (19% de las respuestas). Existe una tendencia emergente en los operadores de servicios de salud y los CSIRT del sector sanitario van más allá del intercambio de información para organizar capacidades IRC. En la práctica significa hacer uso de los esquemas de informes existentes (como los informes de la Directiva NIS) y organizar comunidades sectoriales de confianza de usuarios, que permita intercambiar, de forma segura, tanto ex-ante como información de incidentes ex-post, aprovechando las herramientas existentes y las soluciones automatizadas.

- El establecimiento de normas específicas del sector que regulen los requisitos de seguridad y responsabilidades (17% de las respuestas). Reglamentos específicos del sector sanitario, incluyendo directrices y requisitos para la notificación y gestión de incidentes, ayudan a impulsar la mejorar las capacidades a nivel sectorial. Un ejemplo de regulación sectorial es el Reglamento (UE) 2017/745 sobre productos sanitarios, que obligó a los fabricantes de dispositivos médicos a considerar los riesgos de ciberseguridad en su proceso de producción.

- El establecimiento de convenios de cooperación entre las Administraciones públicas y los operadores

de servicios sectoriales (13% de las respuestas). El apoyo de los equipos de respuesta a incidentes de seguridad informática (CSIRT) Nacionales al desarrollo de las capacidades CSIRT Sectoriales de Salud tiene un gran valor añadido porque aprovecha la experiencia existente. Los operadoresde servicios sectoriales pueden beneficiese de la experiencia y el conocimiento de los equipos CSIRT nacionales y otros sectoriales, mediante la creación de enlaces, el intercambio de conocimientos técnicos, el asesoramiento de expertos o programas de formación específicas. Por ejemplo, una iniciativa novedosa, anterior a la Directiva NIS, es el caso del NCSC holandés proporcionó incentivos y directrices para apoyar la creación de Equipo de Respuesta a Emergencias Informáticas (CERT).

- El establecimiento de alianzas público-privadas (11% de las respuestas). Las asociaciones empresariales desempeñan un papel clave en ciertas actividades relacionadas con la respuesta a incidentes informático (IR). Por ejemplo, pueden fomentar el intercambio de experiencias sobre el uso de herramientas comerciales o de acceso abierto, especialmente aquellas automatizadas dentro de un sector específico, como el sanitario, para beneficiarse de la experiencia acumulada en el sector y acelerar la consolidación de las entidades IR recién creadas.



- Las razones y factores habilitantes que conducen a la creación de una Sectorial de Salud. En el caso de CSIRT en los Países Bajos, las principales razones que parecen haber llevado a la creación de Z-CERT es la alta tasa de vulnerabilidad de los hospitales en sus sistemas informáticos. Al Sistema Público de Salud holandés (NCSC) solo se le permitía por ley proporcionar servicios a operadores de servicios esenciales y vitales, así como al gobierno central. Por lo tanto, sin Z-CERT, la sanidad neerlandesa no tendría acceso a la información pertinente sobre amenazas, especialmente ante el creciente número de ciberataques contra el sector sanitario.

III.2.2. Servicios de los equipos de respuesta.

La segunda conclusión básica que obtiene la Agencia es que los equipos CSIRT sectoriales de salud dan servicios más adaptados a las necesidades del sector que los CSIRT Nacionales ya que tienen en cuenta las especificidades y necesidades del sector sanitario. Los CSIRT Sectoriales de Salud ofrecen las siguientes ventajas:

- Servicios especializados para tratar las amenazas, vulnerabilidades e incidentes específicos del sector.
- Conocimiento y experiencia específicos en dispositivos médicos, sistemas de TI médicos, así como amenazas e incidentes relacionados con el sector salud.
- Proporcionan experiencia sectorial al CSIRT Nacional.
- Asisten a los operadores de servicios del sector salud en la respuesta a incidentes.
- Coordinan los sistemas interconectados en el sector salud.
- Coordinan las vulnerabilidades con proveedores de sistemas/dispositivos específicos del sector.

En general, podemos concluir que los encuestados creen que los CSIRT sectoriales pueden ofrecer más y más profundos conocimiento especializado sobre amenazas específicas del sector y tecnología operativa, así como trabajo en red con organismos y organizaciones sectoriales de salud. Evidentemente, esta observación también depende de la escala y capacidades del CSIRT nacional.

La respuesta a incidentes en el sector salud tiende a ser a menudo reactiva, es decir, dirigida a responder a amenazas o ataques contra los sistemas del CSIRT, en lugar de proactivas, es decir, dirigidas a prevenir inciden-

tes y reducir su impacto negativo cuando ocurren. Esta naturaleza reactiva parece deberse a una comunicación y colaboración insuficientes entre las diferentes partes intervinientes en una situación de vulnerabilidad por ataque (CSIRT nacionales/sectoriales, clientes finales, operadores de servicios esenciales etc.). Los CSIRT sectoriales están en una mejor situación para facilitar y fomentar un enfoque más proactivo a las respuestas a incidentes informáticos, ya que tienen un conocimiento profundo y una estrecha relación con las principales empresas sectoriales. También pueden apoyar la simplificación del intercambio de información, especialmente con los OES.

III.2.3. Herramientas y procedimientos de respuesta a incidentes.

La tercera conclusión que obtiene la Agencia es que los principales recursos y herramientas existentes para apoyar el desarrollo de las capacidades de respuesta a incidentes (IRC) en el sector de la salud son las relacionadas con los marcos compartidos de incidencias, la clasificación y modelos de amenazas, actividades de capacitación y educación y una red de responsables de respuesta a incidentes[13].

A. Recursos adecuados. Hay 5 tipos diferentes de herramientas posibles según el servicio que ofrecen dentro del alcance de las responsabilidades de los CSIRT:

1. Herramientas de gestión de incidencias de seguridad de la información (seguimiento, detección y análisis de situaciones).

2. Herramientas de gestión de incidentes de seguridad de la información (informes de incidentes de seguridad, análisis de incidentes de seguridad, pruebas forenses, mitigación y procedimientos de recuperación, coordinación de incidentes de seguridad de la información y apoyo en las crisis).

3. Herramientas de gestión de vulnerabilidades. Estos servicios abarcan el descubrimiento de vulnerabilidades / investigación, admisión de informes de vulnerabilidad, análisis de vulnerabilidad, coordinación de vulnerabilidad, divulgación de vulnerabilidades y, por último, respuesta a vulnerabilidades.

4. Herramientas de conocimiento de la situación. Esta categoría consta de los siguientes subtipos: análisis-síntesis y comunicación.

5. Herramientas de transferencia de conocimiento. Implica concienciación, formación y educación, y, herramientas de asesoramiento técnico y político.

Es importante tener en cuenta que las organizaciones que tienen menos recursos para desarrollar respuesta frente a ataques informáticos son más propensas a buscar soluciones externas. Esto puede conducir a algún tipo de estandarización incidental de las prácticas de seguridad que impactan en el desempeño general de los usuarios de herramientas externalizadas.

Finalmente, de acuerdo con las respuestas de la encuesta, los principales recursos y herramientas existentes para apoyar la el desarrollo de capacidades IRC de los operadores de servicios en el sector de la salud son: los marcos compartidos de incidentes clasificadas y la experiencia acumulada de los modelos de amenazas sufridas (24 % de las respuestas), las actividades de capacitación y educación frente a las amenazas (24 %), y una red de actores de respuesta a incidentes a nivel nacional o sectorial de salud para intercambiar buenas prácticas sobre intercambio de información, capacidades y cooperación (20%).

B. Procedimientos. Además de los tipos de herramientas señalados, existen otras variantes que deben considerarse para garantizar un manejo exitoso de los incidentes. En este sentido, la claridad y disponibilidad de los procedimientos que se establecen son clave en el curso de la respuesta a incidentes. Los procedimientos para el uso de las herramientas deben estar siempre escritos y al alcance de los responsables que responden a la amenazas e incidentes.

Por ejemplo, después de la recopilación del incidente informado, los equipos CSIRT deben definir y aplicar algún tipo de clasificación de la información[14]. Tras la clasificación de los casos, debe existir un documento formal en el que se indiquen las pautas de creación y gestión de incidentes. En este sentido, un plan demasiado complicado o impreciso puede disuadir de reaccionar con rapidez ante un ciberataque a nivel organizativo o impedir que aumente la concienciación sobre posibles amenazas.

13 Según el artículo 9 de la Directiva NIS, los CSIRT son responsables de la gestión de riesgos e incidentes de acuerdo con un proceso bien definido y con los recursos adecuados.

14 Según la Directiva NIS, "Para facilitar la cooperación, los CSIRT promoverán la adopción y el uso de prácticas comunes o normalizadas para (i) procedimientos de gestión de incidentes y riesgos; (ii) esquemas de clasificación de incidentes, riesgos e información que ellos mismos definan"

Se deprende del estudio que más de la mitad de los CSIRT del Sector Salud ofrecen procedimientos claros. Así, destacan que sus organizaciones tienen procedimientos operativos estándar (POE) y que su organización hizo uso de una plantilla de notificación de incidentes. Esta recopilación de información es importante, ya que el uso de una plantilla indica permite a los CSIRT clasificar la información recopilada.

En relación con la respuesta a incidentes en situaciones de crisis transfronterizas, mientras que la mitad de los encuestados (47%) declaró que existen procedimientos específicos para atender incidentes transfronterizos, señalan que no existe un procedimiento claro sobre cómo se tratan. En algunos casos, hay un enfoque sectorial o nacional, en otros casos se realiza a través de un tercero. Además, destacan que en el 60 % de los casos, sus CSIRT tenían establecidas medidas para informar a los responsables relevantes (autoridades nacionales y OES) de países miembros sobre un incidente que pueda afectarlos; el 47% afirma que informaría a otras partes interesadas a través de un punto de contacto (un tercero de confianza), mientras que solo el 13 % confiaría en un contacto directo (comunicándose con los actores relevantes utilizando su información de contacto directo, sin pasar por un intermediario. En particular, si bien estas recomendaciones son de aplicación general, cada CSIRT de salud tiene necesidades específicas, que deben reflejarse en la confección de sus herramientas y procedimientos.

Por último, otro elemento clave a considerar es el uso y mantenimiento de las soluciones CSIRT: las herramientas y los procesos deben administrarse, probarse y actualizarse para lograr una protección completa contra las agresiones, así como mantener una formación complementaria continua del personal afectado.

III.2.4. Desarrollo de las respuestas a incidentes.

La cuarta conclusión que el estudio ha puesto de manifiesto es que las principales fuerzas que impulsan el desarrollo de las respuestas a incidentes (IR) de los CSIRT son las siguientes: las normas específicas sobre los requisitos de seguridad, las responsabilidades de las organizaciones, y el intercambio de información relacionada con las respuestas a incidentes.

La madurez de un CSIRT se define como la medida de su capacidad en términos de estructura, personas, procesos y tecnologías para afrontar con éxito una respuesta a un incidente informático. Sus capacidades deben garantizar que la organización pueda realizar sus actividades y funciones de manera consistente, así como ser capaz de desarrollar continuamente estas capacidades.

En este sentido, ENISA ha desarrollado un modelo de evaluación de la madurez que se puede utilizar para evaluar las capacidades de los CSIRT. Sobre la base de este modelo de madurez, hay tres cuestiones para tener en cuenta y que influyen en el desarrollo de las capacidades de los CSIRT: en primer lugar, el desempeño ininterrumpido de tareas y procedimientos; en segundo lugar, una cultura laboral de mejora continua de las capacidades del CSIRT (seguimiento del desempeño de tareas, por ejemplo), para proporcionar una capacitación continua al equipo de personas (para formar y actualizar la experiencia del equipo). Todo ello con el fin de poner en marcha políticas, procedimientos y flujos de trabajo que apoyen los objetivos y tareas del equipo. Por último, estos objetivos solo pueden ser alcanzables si el CSIRT cumple los siguientes requisitos previos: llevar un tiempo en funcionamiento, tener un presupuesto suficiente y tener una baja tasa de rotación de miembros del personal.

La madurez de los CSIRT se puede medir y clasificar en tres niveles:

- **Nivel de Madurez Básico:** el equipo CSIRT coordina la gestión de incidentes, tiene un mínimo soporte en cuanto a su existencia, es fácilmente accesible y cuenta con un proceso básico de gestión de incidentes.
- **Nivel de Madurez Intermedio:** el CSIRT coordina la gestión de incidentes, y también permite actividades conjuntas adicionales (como la gestión de vulnerabilidades), tiene una base desarrollada, con descripciones detalladas de las herramientas, procesos y recursos humanos relevantes.
- **Nivel de Madurez Avanzado:** el CSIRT coordina la gestión de incidentes, a la vez que apoya de forma fiable actividades conjuntas adicionales, como el intercambio de amenazas y la alerta temprana datos y manejo de vulnerabilidades. Esto implica que el CSIRT tiene bien descrito, aprobado, y evaluados sus procesos, herramientas y los recursos humanos asignados.

El modelo de evaluación ofrece una imagen clara de la madurez de un CSIRT. Según este modelo, más del 90% de todos los CSIRT nacionales o equipos gubernamentales de ámbito nacional alcanzaron el nivel de madurez básico como mínimo, y, por término medio, estuvieron a punto de alcanzar el nivel de madurez Intermedio ya que sólo necesita formalizar los procedimientos ya existentes[15].

Sin embargo, la consulta realizada reveló que solo el 40% de los CSIRT de Salud utilizan una metodología específica de evaluación de la madurez del CSIRT para

respaldar el desarrollo de las capacidades de respuesta a incidentes dentro de su sector. De estos, la mayoría se basó en el modelo SIM3 (Security Incident Management Maturity Model) y, en menor medida, en la herramienta de madurez del CSIRT nacional disponible en su país. No obstante, a juicio de la Agencia todas las metodologías se consideran pertinentes para mejorar la madurez de los CSIRT.

Además, señalaron que los factores clave que facilitan el desarrollo de la madurez de CSIRT sanitarios y/o sus capacidades de respuesta (IR) dependen principalmente de lo siguiente:

- El establecimiento de regulaciones específicas del sector que aclaren los requisitos de seguridad y responsabilidades (18% de las respuestas).
- La difusión de información sobre amenazas, el intercambio de buenas prácticas y experiencias aprendidas (16% de las respuestas).
- En menor medida, el establecimiento de acuerdos de cooperación entre instituciones nacionales y actores sectoriales (13% de las respuestas).

III.2.5. Retos y lagunas de los equipos de respuesta a incidentes de seguridad informática.

Las quinta conclusión que obtenemos del estudio es que a la hora de dar respuesta a incidentes, los equipos CSRT de salud se encuentran con tres problemas: en primer lugar, la falta de cultura de seguridad entre los Operadores de Servicios Esenciales (OES); en segundo lugar, el hecho de que la gestión (y la seguridad) de la infraestructura de la infraestructura informática de las OES se suele subcontratar; y, por último, la falta de herramientas y canales de cooperación establecidos con los equipos de respuesta a incidentes de OES.

A. Desafíos de ciberseguridad de los OES.

En general, los operadores sanitarios se enfrentan a complicaciones específicas en el ámbito de la ciberseguridad y la respuesta a incidentes, debido a la naturaleza de los servicios del sector sanitario. En consecuencia, la eficacia de los CSIRT sanitarios es menor que en otros ámbitos.

A continuación, señalamos los principales problemas a los que se enfrentan los proveedores de servicios sanitarios:

- **Equipo:** sistemas antiguos sin diseño ciberseguro. Los sectores tradicionales, incluido el sanitario, son más vulnerables a los ciberataques ya que los sistemas y equipos tienen una vida útil prolongada (15 años de promedio). En muchos casos no fueron diseñado para hacer frente a ciberataques.

Ello ha dado lugar a un aumento constante del número de vulnerabilidades detectadas en los proveedores de dispositivos digitales y en los fabricantes de hardware. Ha obligado a los hospitales a actualizar y adaptar sus sistemas en muy poco tiempo dada la alta vulnerabilidad derivada de la obsolescencia de la tecnología informática a lo largo de su ciclo de vida. De ahí que el ritmo de las actualizaciones se vea rápidamente superado por el de la evolución de la tecnología informática. Además, esta dependencia de los proveedores se ve acentuada por la adopción de dispositivos IoT por parte de los proveedores del sector sanitario, lo que amplía enormemente las áreas que pueden ser atacadas[16]. El hecho de que esta

15 En el marco del modelo ENISA, alcanzar el nivel básico de madurez implica que el CSIRT analizado está operativo, con un proceso básico de gestión de incidentes en funcionamiento, su información disponible para otros equipos, sus servicios son definido de acuerdo con el RFC2350, y el equipo ha alcanzado un nivel adecuado de madurez. https://www.enisa.europa.eu/publications/study-on-csirt-maturity

16 l Internet de las cosas (IoT) es el proceso que permite conectar los elementos físicos cotidianos al Internet: desde los objetos domésticos comunes, como las bombillas de luz, hasta los recursos para la atención de la salud, como los dispositivos médicos; las prendas y los accesorios personales inteligentes; e incluso los sistemas de las ciudades inteligentes. Los dispositivos del IoT que se encuentran dentro de esos objetos físicos suelen pertenecer a una de estas dos categorías: son interruptores (es decir, envían las instrucciones a un objeto) o son sensores (recopilan los datos y los envían a otro lugar).

serie de dispositivos esté estrechamente interconectada no hace sino incrementar el problema y el impacto potencial de las amenazas. Al mismo tiempo, los profesionales sanitarios suelen eludir la seguridad para ofrecer una mejor atención a los pacientes.

En esta línea, algunos problemas recurrentes son las configuraciones de encriptación inadecuadas, y la incapacidad para compartir e intercambiar información de salud segura con terceros y socios transfronterizos (no existen herramientas sofisticadas de seguridad de datos en el sector sanitario).

■ **La complejidad organizativa se une a la notificación de incidentes.** En estrecha relación con el apartado anterior, la complejidad organizativa supone un reto para la ciberseguridad de los proveedores sanitarios. La amplia cadena de suministro del sector sanitario implica a muchas partes interesadas, lo que puede provocar efectos en cascada en medio de una situación crítica. Concretamente, los nichos organizativos, así como las disparidades entre los miembros del hospital son riesgos recurrentes.

Además, la coordinación de la respuesta a un incidente se ve muy afectada por esta complejidad. En el curso de un incidente, los planes de respuesta demasiado complicados, que involucran a muchas partes interesadas etc. retrasan la eficacia del procedimiento, ya que cada miembro del equipo no siempre es consciente de su papel en el proceso. Como resultado, el sector sanitario corre el riesgo de que transcurra mucho tiempo entre un ataque, detección y respuesta.

- **Intercambio de información.** El estudio ha puesto de manifiesto la falta de intercambio de información y buenas prácticas a nivel sectorial sanitario y entre países[17].

- **Falta de experiencia.** Hay una falta de expertos lo suficientemente calificados en el sector sanitario. El equipo adquirido por los hospitales no protegerá de un operador de ataques cibernéticos si se usa de manera inadecuada o el personal no ha sido capacitado adecuadamente.

- **Falta de conciencia de seguridad.** Hay poca conciencia sobre los riesgos cibernéticos en el sector de la salud y su impacto potencial en la organización hospitalaria. En general, los profesionales de la salud no son conscientes de las consecuencias de conductas de riesgo, motivadas por la falta de políticas de refuerzo de protocolos de seguridad[18].

- **Sistemas de funcionamiento ininterrumpido.** En el sector sanitario es difícil aplicar determinados procedimientos de ciberseguridad en tiempo real, sin apagado de los sistemas y de los equipos. Por ejemplo, pocas infraestructuras informáticas sanitarias podrían desconectarse sin afectar el cuidado o, incluso la vida de los pacientes y, por tanto, al funcionamiento real de los hospitales o centros sanitarios.

B. Desafíos de los equipos de respuesta a incidentes de seguridad informática.

Dentro de este panorama, los equipos CSIRT de Salud consultados para el estudio destacaron que los principales desafíos que se enfrentan cuando se colabora con OES en el sector de la salud suelen ser los siguientes, por orden de importancia:

- Falta de cultura de seguridad entre los operadores de servicios esenciales.

- La gestión y la seguridad de la infraestructura informática de los operadores de servicios esenciales.

- Falta de herramientas y canales de cooperación establecidos con operadores de servicios de equipos de respuesta a incidentes.

- Falta soporte de cobertura de incidencias 24/7.

- Cuestiones de recursos o experiencia.

La conclusión es que todos los desafíos enumerados por los equipos CSIRT de Salud consultados están estrechamente relacionados con los desafíos que tienen las propias OES.

17 Cabe mencionar de nuevo el H-ISAC, que facilita la transferencia de conocimientos en todo el mundo a través de cumbres educativas, seminarios electrónicos, talleres y conferencias, apoyando así el intercambio de información y la creación de relaciones que puedan contribuir a que el sector sanitario sea más resistente y proactivo frente a futuros ciberataques.

18 Esto lo ha demostrado la reciente pandemia por COVID. Necesariamente la digitalización aumentó en el sector de la atención sanitaria que no se acompañó con un aumento en procedimientos técnicos relacionados con la ciberseguridad. El estudio concluye que la falta de conciencia es en parte debido a una inadecuada comunicación de riesgos por parte de la dirección de los hospitales.

En particular, el 60% de los consultados señalaron la ausencia de un equipo CSIRT sectorial de salud específico, por lo que en estos casos no hay solapamientos entre las responsabilidades y servicios de los CSIRT nacionales y los de los CSIRT sectoriales de salud. Sólo el 13% de los entrevistados señalaron que existía un solapamiento entre los CSIRT nacionales y los sectoriales sanitarios.

En cuanto al trabajo interno de los CSIRT, los participantes en la consulta explicaron que los retos recurrentes relacionados con el personal en el contexto de los equipos de respuesta a incidentes incluyen la falta de personal, la falta de conocimientos y aptitudes y la elevada rotación de personal, mientras que los retos organizativos se refieren a la falta de definición formal de responsabilidades y funciones.

IV. Reflexiones finales.

En general, los distintos informes de la Agencia han concluido que los equipos CSIRT sectoriales de Salud aún son escasos en un panorama donde los operadores de servicios esenciales de salud necesitan apoyo especializado en sus actividades de respuesta a incidentes informáticos. Además, los puntos de vista compartidos por las partes consultadas subrayaron el gran potencial de los CSIRT sanitarios para prestar este apoyo, en particular en iniciativas de intercambio de información. Sobre la base de esta área clave de oportunidades y de las necesidades expresadas por los OES, han surgido las siguientes recomendaciones a los Estados miembros.

IV.1. Mejorar y facilitar la creación de los equipos CSIRT sectoriales sanitarias.

Aunque existe una tendencia a desarrollar CSIRT sectoriales y colaboraciones entre CSIRT sectoriales por parte de los OES de salud, todavía son pocos los gobiernos que cuentan con CSIRT de salud o que tienen la intención de crearlo. En general las capacidades de respuesta a incidentes son gestionadas por los principales OES y supervisadas por el CSIRT nacional o gubernamental, dejando la coordinación de las respuestas a incidentes y las actividades de intercambio de información a de información a partes con menos experiencia en esta área de intersección entre la ciberseguridad y la atención sanitaria.

• Primera recomendación. Dirigida a las Autoridades Nacionales de ciberseguridad de la UE.

Deben realizarse esfuerzos para facilitar la financiación, orientación (en relación con la capacidad construcción, intercambio de información, sensibilización) y cooperación para garantizar la creación de CSIRT Sectoriales de Salud.

IV.2. Aprovechar la experiencia de equipos CSIRT sectoriales sanitarias para ayudar a OES a desarrollar sus capacidades de respuesta.

Los operadores de servicios esenciales de salud enfatizaron en la necesidad de orientación, dirección y desarrollo de capacidades cuando se trata de dar respuesta a cualquier incidente. La dificultad se centra en que la respuesta a los incidentes en el sector sanitario tiende a depender más de los servicios reactivos que de los proactivos, debido a la falta de una capacidad coordinada de respuesta. Concretamente, los operadores de servicios esenciales de salud necesitan ayuda para identificar las experiencias adquiridas de incidentes pasados en el sector. Al mismo tiempo, la falta de conocimientos sectoriales específicos de los equipos CSIRT nacionales les impide desempeñar esta función de coordinación que los CSIRT de salud pueden asumir.

Por ello, los CSIRT sanitarios deberían estar facultados para asumir la función de apoyo a los OES en materia de respuesta a incidentes, fomentando la organización y la puesta en común de capacidades de respuesta a incidentes de forma más proactiva.

• Segunda recomendación. Dirigida a las Autoridades nacionales de Ciberseguridad de la UE, Sectoriales y/o Nacionales CSIRT.

Esta función incluiría las siguientes responsabilidades:

- Promoción de servicios especializados para hacer frente a amenazas, vulnerabilidades e incidentes específicos del sector.
- Difusión de conocimientos y experiencia específicos sobre dispositivos médicos y sistemas informáticos médicos, así como sobre amenazas e incidentes relacionados con el sector sanitario en tiempo real.
- Proporcionar conocimientos sectoriales al CSIRT nacional, asistir a los operadores no regulados del sector sanitario en la respuesta a incidentes, coordinar los sistemas comprometidos en múltiples emplazamientos del sector sanitario.
- Coordinación de la vulnerabilidad con los proveedores de sistemas y dispositivos específicos del sector sanitario.

Estas actividades abordan los principales retos tanto de los OES sanitarios como de los CSIRT. Además, el cumplimiento de estas actividades requerirá un gran esfuerzo por parte de los CSIRT sanitarios, así como el desarrollo de conocimientos especializados y la cooperación con los CSIRT nacionales e internacionales.

Para lograrlo, se proponen las siguientes medidas para mejorar las capacidades de los CSIRT sanitarios:

- Establecimiento de normativas sectoriales específicas que aclaren los requisitos y responsabilidades en materia de seguridad (como directrices y requisitos para la notificación y gestión de incidentes).
- Establecimiento de acuerdos de cooperación entre los agentes nacionales y sectoriales (mediante la designación de un funcionario de enlace), el intercambio de conocimientos técnicos, el asesoramiento de expertos o la formación a medida).
- Establecimiento de un canal de comunicación directo y fluido con los OES.
- Participación de asociaciones público-privadas, que pueden acelerar el desarrollo de los IR, OES y CSIRT sanitarios.

IV.3. Potenciar el papel de las CSIRT sanitarios en actividades de intercambio de información.

La última recomendación de la Agencia Europea subraya la importancia de capacitar a los CSIRT de salud para que compartan información entre las OES. La aparición orgánica de CSIRT sanitarios, como el Centro de Análisis e Intercambio de y Análisis de la Información Sanitaria (H-ISAC), apunta a la necesidad de los OES de intercambiar información, sin pasar por los sistemas centralizados nacionales que no disponen de la capacidad necesaria para ello. Los sistemas nacionales centralizados que carecen de conocimientos sectoriales específicos y pueden crear pasos adicionales innecesarios en el intercambio de información.

• Tercera recomendación dirigida a Autoridades Nacionales de Ciberseguridad de la UE, Red de equipos de respuesta a incidentes de seguridad informática y Equipos de respuesta a incidentes de seguridad informática Sectoriales y/o Nacionales.

Los CSIRT sanitarios deben contribuir a agilizar las dificultades asociadas al intercambio de información sobre incidentes, especialmente complicadas en el sector sanitario. Concretamente, los CSIRT sanitarios deben recibir apoyo para desarrollar actividades de intercambio de información, que debe incluir, entre otras cosas, la difusión de información sobre amenazas (tanto ex ante como ex post), intercambio de buenas prácticas y experiencias adquiridas, así como información sobre formación y entrenamientos para la capacitación de los OES.

ANEXO[19].

Estados	Resumen del enfoque nacional para dar respuesta a incidentes (IR) en el sector salud	Sector Salud	Estado desarrollo
Austria	CERT.at es el CERT nacional de Austria. En el caso de ataques significativos en línea contra la infraestructura sanitaria austríaca.	No	Previsto desarrollado
Bélgica	El CERT.be, es el servicio operativo de la Centro para la Seguridad Cibernética de Bélgica (CCB). No tiene un CSIRT dedicado entidad para el sector salud.	No	N/A
Bulgaria	CERT Bulgaria es el Equipo de respuesta a incidentes de seguridad. Bulgaria. Creando actualmente CSIRT Sectoriales para facilitar la aplicación de la Directiva NIS. No cuenta con un CSIRT Sectorial de Salud.	No	En preparación
Croacia	El CERT Nacional es responsable de prevención de ciberamenazas y protección de la seguridad de los sistemas de información públicos. No tiene CSIRT Sectorial de Salud dedicado.	No	Previsto desarrollado
Chipre	CSIRT-CY es la Seguridad Informática Nacional Equipo de respuesta a incidentes. No existe una entidad dedicada al sector salud.	No	N/A
República Checa	CSIRT.CZ es el CSIRT Nacional de la República Checa. No tiene un CSIRT Sectorial de Salud.	No	N/A
Dinamarca	En Dinamarca, existe un CSIRT del sector sanitario, la Autoridad Danesa de Datos que se encuentra actualmente en fase de desarrollo.	No	En preparación
Estonia	CERT-EE es una organización responsable de la gestión de incidentes de seguridad. No hay entidad dedicada al sector salud.	No	N/A
Finlandia	El Centro Nacional de Seguridad Cibernética de Finlandia (NCSCFI) es responsable de la supervisión de todos CSIRT. Tiene una eficiente autoridad supervisora del sector salud. No hay planes concretos par aun sector CSIRT específico sanitario.	No	N/A
Francia	Francia tiene un CSIRT Sectorial dedicado para el sector salud, CERT Santé (anteriormente llamado Acompañamiento Cyber sécurité des Structures de Santé), vigente desde 2017.	SI	Desarrollado
Alemania	CERT-Bund (Respuesta de Emergencia Informática). No hay una entidad dedicada al sector de la salud.	No	N/A
Grecia	GR-CSIRT es el equipo cibernético de defensa, respuesta a incidentes y Operaciones. No tiene un CSIRT Sectorial de Salud.	No	N/A
Hungría	Hay tres unidades organizativas en la Seguridad Cibernética Nacional. Launidad Gov CERT Hungary es responsable de la gestión de incidentes. No existe una entidad dedicada a la salud.	No	N/A

19 Fuente elaboración propia a partir de los informes precitados de ENISA. La siguiente tabla proporciona un resumen del diseño y la configuración de respuesta a incidentes IR sectorial, a nivel europeo. La información relacionada con los siguientes 12 Estados miembros se recopiló a través de la encuesta de ENISA: Francia; Bulgaria; República Checa; letonia; Austria; Croacia; Finlandia; Estonia; Chipre; Hungría; España; Dinamarca. Los hallazgos restantes provienen de revisión de la literatura científica.

Irlanda	CSIRT-IE es el organismo dentro de la Cibernética Nacional Security Center (NCSC) asiste a los incidentes de seguridad cibernética a nivel nacional. El CSIRT-IE también actúa como un punto de contacto nacional para ataques cibernéticos que involucran entidades de atención médica dentro de Irlanda. No hay entidad dedicada al sector salud.	No	N/A
Italia	Equipo de Respuesta a Incidentes de Seguridad Informática se encuentra dentro del Departamento de Seguridad. No existe una entidad dedicada al sector salud.	No	N/A
Letonia	No cuenta con un CSIRT Sectorial de Salud.	No	N/A
Lituania	No cuenta con un CSIRT Sectorial de Salud.	No	N/A
Luxemburgo	Hay dos CSIRT nacionales en Luxemburgo. Él Centro de respuesta a incidentes informáticos de Luxemburgo (CIRCL) y GOVCERT, que dan una facilidad de respuesta a las amenazas de seguridad informática e incidentes del sector sanitario. HealthNet-CSIRT (Equipo de Respuesta a Incidentes) es el punto de contacto para procesamiento de incidentes informáticos encontrados por diversos actores activos en el ámbito de la salud.	SI	Desarrollado
Malta	No cuenta con un CSIRT Sectorial de Salud.	No	N/A
Países Bajos	El Centro Nacional de Ciberseguridad (NCSC.NL) es responsable de la coordinación de medidas de respuesta a incidentes para las instituciones y entidades relacionadas con infraestructuras críticas. Cuentan con un CSIRT (Z-CERT) que es un Equipo de Respuesta a Emergencias Informáticas) específicamente para instituciones del sector sanitario.	SI	Desarrollado
Polonia	Los tres CSIRT nacionales son el Computer Security Incident Response Team (CSIRT GOV), el Equipo de Respuesta a Incidentes de Seguridad Seguridad Informática del Ministerio de Defensa polaco (CSIRT MON) y el de Respuesta a Emergencias Informáticas CERT-POLSKA, que contribuyen a garantizar la ciberseguridad a nivel ciberseguridad a nivel nacional. No existe una entidad dedicada al sector de la salud.	No	N/A
Portugal	El CERT.PT es un servicio integrado en su Centro Nacional de Ciberseguridad que coordina la respuesta a incidentes relacionados con el ciberespacio nacional. No cuenta con un CSIRT Sectorial de Salud.	No	N/A
Rumanía	No hay ninguna entidad dedicada al sector de la salud.	No	N/A
Eslovaquia	El Centro Nacional de Ciberseguridad SK-CERT realiza actividades nacionales y estratégicas en el ámbito Ciberseguridad. No existe una entidad dedicada al sector sanitario.	No	N/A
Eslovenia	No cuenta con una entidad dedicada al sector sanitario.	No	N/A
España	INCIBE-CERT es el centro de respuesta a incidentes de seguridad de seguridad de referencia para ciudadanos y entidades operado por el Instituto Nacional Ciberseguridad (INCIBE), dependiente del Ministerio de Economía y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. No existe una entidad dedicada el sector sanitario.	No	N/A
Suecia	No cuenta con un CSIRT específico para el sector sanitario.	No	N/A

Lista de abreviaturas

- CERT: Computer Emergency Response Team
- CSIRT: Computer Security Incident Response Teams
- ENISA: European Union Agency for Cybersecurity
- IoT: Internet of Things
- IR: Incident Response
- IRC: Incident Response Capabilities
- IT: Information Technology
- OES: Operators of Essential Services
- SOP: Standard Operating Procedure

V. Bibliografía

- Cabezón Ruiz, S. y Morilla, R.: "Big data en salud: un nuevo paradigma para regular, Un desafío para la justicia social", en Revista Española de Salud Pública. 2021; Vol. 95: 7 de octubre.
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativo a las medidas para un alto nivel común de seguridad de las redes y los sistemas de información en toda la Unión, DO L 194/1,19.7.2016, Bruselas.
- ENISA: Cloud Security foro Healthcare Services (2021). ENISA: CSIRT Capabilities in Halthcare Sector (november 2021). ENISA: Procurement Guidelines for Cybersecurity in Hospitals (2020). ENISA: Pseudonymisation techniques and best practices. (2019). ENISA: Procurement Guidelines for Cybersecurity in Hospitals. (2020). ENISA, CSIRT Capa-

cidades. ¿Cómo evaluar la madurez? Directrices para los organismos nacionales y gubernamentales (2019).

- https://esante.gouv.fr/securite/cert-santé
- https://op.europa.eu/en/publication-detail/-/publication/3b6ad641-d23c-11eb-ac72-01aa75ed71a1
- https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report
- https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework.
- https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware
- Jareño Butron, M. y Arratibel Arrondo, J.A.: "Técnicas para el control del tratamiento masivo de datos personales en el sector público sanitario." Revista Auditoría Pública no 81 enero-junio 2023. Páginas: 180-195.
- Revista de la sociedad española de informática y salud, en 1 39, abril 2020. monográfico: "Ciberseguridad, clave para la transformación tecnológica en salud".