El sector sanitario europeo frente a la ciberamenaza: propuesta de una fiscalización informática.

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 86
Diciembre 2025. Páginas: 109-118

Resumen: 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. Por tanto, los datos personales de salud de los pacientes fueron el objetivo primordial de los ataques. Recordamos que la nueva normativa europea de protección de datos (RGPD), considera esta información como especialmente protegida por las administraciones gubernamentales.

En este trabajo pretendemos analizar las conclusiones derivadas del reciente informe emitido por la Agencia de Ciberseguridad de la Unión Europea (ENISA) en relación con las ciberamenazas del sector sanitario en la UE. Además, hemos tenido en cuenta anteriores informes que complementan este panorama y que han sido objeto de análisis en anteriores trabajos.[1] El informe tiene como objetivo aportar nuevos conocimientos sobre la realidad del sector de la salud mediante el mapeo y el estudio de incidentes cibernéticos desde de 2020 hasta marzo de 2023. Identifica las principales amenazas, actores, impactos y tendencias basándose en el análisis de los ciberataques dirigidos a organizaciones de salud durante los últimos tres años.[2]

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. 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: Ciberamenazas sector sanitario, protección de datos personales salud, ciberseguridad hospitalaria, ENISA.

Abstract: The volume and intensity of cyberattacks in the healthcare sector have increased starting in 2020. Healthcare organizations, in general, and hospitals, in particular, have been a major target for cybercrime, primarily due to the value of the data that can be obtained from an attack, as well as its disruptive impact. Therefore, patients' personal health data was the primary target of the attacks. We recall that the new European data protection regulation (GDPR) considers this information as especially protected by governmental administrations. In this work, we aim to analyze the conclusions derived from the recent report issued by the European Union Agency for Cybersecurity (ENISA) regarding cyber threats in the EU healthcare sector. Furthermore, we have taken into account previous reports that complement this landscape and which have been analyzed in previous works. The report aims to provide new insights into the reality of the health sector by mapping and studying cyber incidents from 2020 to March 2023. It identifies the main threats, actors, impacts, and trends based on the analysis of cyberattacks targeting health organizations over the last three years. There is no doubt that these conclusions will lay the groundwork for the further development of European regulation on health cybersecurity, thereby addressing the technical and legal aspects of the right to privacy of personal health data in the European Union. Ultimately, this is a necessarily interdisciplinary work that requires taking into account the positive law of personal health data protection and the technical aspects of current computer engineering to guarantee these rights in the safest possible way.

Keywords: Healthcare sector cyber threats, personal health data protection, hospital cybersecurity, ENISA.

1 Nos remitimos a nuestros anteriores trabajos: 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; "Bases del modelo de respuesta europeo a incidentes de ciberseguridad informática en el sector sanitario." Diario La Ley, ISSN 1989-6913, Nº 10223, 2023.

2 ENISA THREAT LANDSCAPE: HEALTH SECTOR (January 2021 to March 2023) JULY 2023. ISBN 978-92-9204-638-5 DOI 10.2824/163953 TP-04-23-546-EN-N (En adelante el informe).

I. Introducción.

Desde 2022 el sector sanitario europeo se ha enfrentado a un número importante de ciberincidentes. Los proveedores de atención sanitaria de la UE, especialmente los hospitales, se han visto especialmente afectados. También se observa incidentes contra autoridades, organismos y agencias sanitarias y ataques a la industria farmacéutica. A modo de ejemplo, recordamos el último ciberataque que sufrió un centro sanitario del Estado, el Hospital Clínic Barcelona (5-03-23), y el esfuerzo de la Agencia de Ciberseguridad de Catalunya para el análisis y recuperación de los sistemas de información robados.

El ransomware es la principal amenaza en el sector sanitario, tanto por el número de incidentes como por su impacto en las organizaciones sanitarias. De hecho, el 43% de los incidentes de ransomware van acompañados de una filtración o robo de datos. La mitad del total de incidentes son amenazas contra los datos de las organizaciones sanitarias (violaciones de datos, fugas de datos). Además, los ataques a la cadena de suministro y a los proveedores de servicios de atención médica han causado interrupciones o pérdidas a las organizaciones del sector de la salud. En un reciente estudio de ENISA, la sanidad fue el sector que más incidentes de seguridad declaró relacionados con vulnerabilidades en software o hardware.

Por otro lado, los acontecimientos geopolíticos y la actividad hacktivista aumentaron el número de ataques DDoS contra hospitales y autoridades sanitarias a principios de 2023, alcanzando el 9% del total de incidentes. Esto se debió a un aumento de los ataques DDoS por parte de grupos hacktivistas prorrusos que tenían como objetivo perturbar a los proveedores de atención médica y a las autoridades sanitarias de la UE. Todos los datos indican que esta tendencia continuará en los próximos años.

En términos de impacto, los incidentes observados provocaron principalmente violaciones o robo de datos (43%), interrupciones en los servicios de salud (22%) y otros servicios no relacionados con la salud (26%). Las filtraciones de datos afectaron a entidades sanitarias en el 40% del total de incidentes y, en particular, a hospitales (27%) y atención primaria (8%). La interrupción de los servicios de salud se produjo cuando las entidades de salud (82%) y las autoridades de salud (12%) fueron perturbadas.

Otros impactos incluyen pérdidas financieras, pero este es un impacto difícil de evaluar. El estudio ENISA "NIS Investment 2022" indica que el coste medio de un incidente importante de seguridad en el sector sanitario es de 300.000 euros. Según ENISA, solo el 27% de las organizaciones encuestadas en el sector de la salud tienen un programa de defensa contra ransomware y el 40% de las organizaciones no tienen ningún programa de concienciación sobre la seguridad para el personal. En otra encuesta reciente realizada por el grupo de cooperación NIS, el 95% de las organizaciones de salud encuestadas enfrentan desafíos al realizar evaluaciones de riesgos, mientras que el 46% nunca ha realizado un análisis de riesgos. Estos resultados indican una necesidad apremiante para que las organizaciones de salud apliquen prácticas de ciberhigiene. Estos pueden incluir copias de seguridad cifradas fuera de línea de datos críticos, programas de concientización y capacitación para profesionales de la salud, manejo y parcheo de vulnerabilidades, métodos de autenticación más sólidos, planes de respuesta a incidentes cibernéticos y planes de contingencia.

Todas etas cuestiones han sido tratadas en distintitos informes y protocolos de ENISA y especialmente en el informe "Threat landscape: health sector (January 2021 to March 2023)," antes citado. Los informes tienen como objetivo aportar nuevos conocimientos sobre l realidad del sector de la salud mediante el mapeo y el estudio de incidentes cibernéticos desde de 2020 hasta marzo de 2023. Identifica las principales amenazas, actores, impactos y tendencias basándose en el análisis de los ciberataques dirigidos a organizaciones de salud durante los últimos tres años que seguidamente analizamos.

II. Panorama de las ciberamenazas al sector sanitario de Europa.

El sector sanitario fue seleccionado por la Agencia Europea debido a la importancia para los ciudadanos europeos y la especial protección de los datos de salud.[3] Ya en informes anteriores (Informe ENISA Threat Landscape 2022), apuntó que alrededor del 7% de los incidentes observados tenían como objetivo organizaciones sanitarias. Además, el 32 % de los incidentes con un impacto significativo notificados con arreglo a la Directiva sobre seguridad de las redes y de la información en 2022 fueron incidentes en el sector sanitario de la UE. En este

3 Sobre este particular nos remitimos a trabajos anteriores: 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.

sentido, durante 12 años consecutivos, el sector sanitario registró el coste medio más elevado de una violación de seguridad en todo el mundo.[4]

El informe "Threat landscape: health sector (January 2021 to March 2023") recoge los incidentes cibernéticos dirigidos al sector sanitario desde enero de 2021 hasta marzo de 2023 ("periodo de referencia"). Agrupa incidentes cibernéticos informados públicamente que afectan a varios los siguientes tipos de organizaciones relacionadas con la salud:

- Prestadores de asistencia sanitaria directa (hospitales, atención primaria, asistencia sociosanitaria, asistencia odontológica, servicios de urgencias, salud mental, etc,).
- Laboratorios de referencia de la UE (entidades con actividades de investigación y desarrollo de medicamentos y relacionadas con la salud).
- Industria de productos farmacéuticos.
- Industria productos sanitarios y biotecnología.
- Autoridades, organismos y agencias sanitarias nacionales y de la UE.
- Organizaciones de seguros de enfermedad.
- Centros residenciales de tratamiento y proveedores de servicios sociales.

El informe aplicó la Metodología del Panorama de Amenazas a la Ciberseguridad de ENISA.[5] La recopilación y el análisis de los datos se centraron en los ciberincidentes observados en los Estados miembros de la UE y los países vecinos (Noruega, Suiza y Reino Unido). Los datos recogidos fueron analizados posteriormente por el equipo de panorama de amenazas de ENISA y por expertos externos.

Estos incidentes sirven de base para identificar una lista de amenazas principales y de material de partida para soportar los resultados (tendencias y estadísticas del informe). Los incidentes se analizaron en detalle para identificar sus elementos centrales, proporcionando respuestas a algunas preguntas importantes, como, por ejemplo: cómo se producen los ataques, qué sistemas son el objetivo y qué organizaciones sanitarias son las más afectadas y cómo.

La estructura del informe es la siguiente:

- Introducción. Ofrece una visión general del ámbito de aplicación y del método utilizado para elaborar este informe.[6]
- Amenazas principales. Analiza la actividad observada durante el periodo cubierto por el informe. Proporciona información sobre las principales amenazas y la distribución geográfica de los incidentes observados.
- Actores de la amenaza y motivación. Analiza los tipos de actores que atacan al sector sanitario y analiza su posible motivación.
- Impacto. Analiza la afección en el sector sanitario, las entidades más atacadas, los activos afectados, así como las consecuencias de los incidentes y las amenazas identificadas.
- Conclusiones.

III. Amenazas.

El total de incidentes notificados públicamente por los países miembros de la UE y países vecinos antes citados, en el período de referencia es de 215. Estos incluyen 208 ciberataques al sector sanitario, 5 informes de vulnerabilidades identificadas, pero no necesariamente explotadas y 2 advertencias de actividad potencial que

4 ENISA Threat Landscape 2022, November 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Data retrieved by the Cybersecurity Incident Reporting and Analysis System (CIRAS). https://ciras.enisa.europa.eu/. IBM Cost of a Data Breach Report 2022. https://www.ibm.com/reports/data-breach

5 ENISA Cybersecurity Threat Landscape Methodology, July 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology. No se trata de la lista completa de incidentes ocurridos durante el periodo de referencia. ENISA recopiló una lista de los principales incidentes basándose en inteligencia de fuentes abiertas (OSINT) y en las propias capacidades de inteligencia sobre ciberamenazas de ENISA.

6 ENISA y expertos externos llevaron a cabo una investigación documental en profundidad de la bibliografía disponible procedente de fuentes abiertas, como artículos de prensa, opiniones de expertos, informes de inteligencia, análisis de incidentes e informes de investigación sobre seguridad. El informe ha sido validado y respaldado por el Grupo de Trabajo Ad Hoc de ENISA. Grupo sobre Paisajes de Amenazas a la Ciberseguridad (CTL) y el Grupo de Cooperación NIS (línea de trabajo 12 sobre el sector sanitario). Además, las organizaciones sanitarias de la UE deben notificar los incidentes de ciberseguridad con un impacto significativo a las autoridades nacionales de su país en virtud de la Directiva NIS. Al final de cada año, los informes resumidos sobre estos incidentes son recopilados, anonimizados, agregados y analizados por ENISA. Debido a su carácter anónimo, estos informes no pueden combinarse con los incidentes recogidos por OSINT, ya que existe el riesgo de que se dupliquen los incidentes. No obstante, ofrecen una imagen complementaria y se presentarán como información adicional a lo largo del informe.

afecta al sector sanitario.

En general, el informe concluye que se produce un número estable de incidentes, con una posible tendencia en aumento en 2023. De hecho, los ataques de denegación de servicio (DoS) dirigidos a varios hospitales en los Países Bajos y España (enero de 2023) y en Dinamarca y Suecia (febrero de 2023) representan una gran parte de la actividad observada durante el primer trimestre de 2023.

Este número de incidentes puede verse afectado por varios factores para tener en cuenta:

Uno. Un aumento en el número de ciberataques notificados no significa necesariamente que el número de ataques haya aumentado realmente o que el impacto de los ataques esté aumentando. Dicho aumento puede producirse a medida que un sector madura en términos de detección y notificación de incidentes, lo que puede deberse al efecto de la obligación legal de notificar incidentes en virtud de la legislación europea o nacional.

Dos. Otra posibilidad es que la atención de los medios de comunicación o de los ciudadanos se centre en un sector concreto durante un periodo de tiempo determinado. Este fue especialmente el caso del sector sanitario durante la pandemia de Covid-19. En este caso, un ciberataque puede impedir que un hospital atienda a los pacientes, lo que puede poner en peligro su bienestar y seguridad.

Gráfico 1.
Mapa de incidentes dirigidos a organizaciones sanitarias en Europa (enero 2021 a marzo 2023)[7].

7 El informe hace hincapié en que las diferencias en el número de incidentes por país son difíciles de interpretarse, ya que pueden verse afectadas por el tamaño de la población o por diferencias en la capacidad de notificación en países concretos o por el propio proceso de recopilación de datos. Lo que sí concluye categóricamente es que existen ciberincidentes dirigidos indiscriminadamente al sector sanitario europeo.

Las conclusiones más importantes, a nuestro juicio, son las siguientes:

1. Existen ciberincidentes dirigidos indiscriminadamente al sector sanitario europeo. Las diferencias en el número de incidentes por país son difíciles de interpretarse, ya que pueden verse afectadas por el tamaño de la población o por diferencias en la capacidad de notificación en países concretos o por el propio proceso de recopilación de datos.

2. La mayoría de los incidentes afectaron a proveedores de asistencia sanitaria (53%) y especialmente a hospitales europeos (42% del total de incidentes). Le siguieron las autoridades, organismos y agencias sanitarias y los ataques a la industria farmacéutica.

3. Los tipos de amenazas dirigidas al sector sanitario europeo (mayoritariamente ransomware y las amenazas relacionadas con los datos personales de salud). El sector sanitario depende en gran medida de datos de carácter personal y sensible, por lo que su posible divulgación tendría graves jurídicas. Evidentemente, se trata de un objetivo atractivo para los ciberdelincuentes, que aprovecharían la oportunidad de rentabilizar sus actividades mediante la extorsión bajo la amenaza de divulgación. Así lo corroboran los resultados en la que el ransomware y las amenazas relacionadas con los datos ocupan los primeros puestos.

4. ENISA ha debatido ampliamente los efectos de la pandemia en el panorama general de las ciberamenazas y señala que en 2020 y 2021, se dio un repunte de los incidentes no maliciosos, ya que la pandemia COVID-19 se convirtió en un multiplicador de los errores humanos y las desconfiguraciones del sistema, hasta el punto de que la mayoría de las brechas en 2020 fueron causadas por errores.[8] A esto se añaden los ataques a la cadena de suministro en 2021, ya que estas vulnerabilidades también estaban presentes en los proveedores sanitarios. En 2022, lo que marcó el panorama de amenazas para el sector fue el aumento de los ataques de ransomware tanto en Europa como a nivel mundial. El ransomware sigue desempeñando un papel clave en 2023 para el sector sanitario, junto con la tendencia emergente de ataques DDoS dirigidos a organizaciones sanitarias.

IV. Actores de las amenazas y motivación.

El informe de ENISA que analizamos junto a otros emitido por la Agencia (ENISA Threat Landscape 2021 y ENISA Threat Landscape 2022), consideran cuatro categorías principales de actores de amenazas a la ciberseguridad: ciberdelincuentes, hackers a sueldo, actores patrocinados por el Estado y hacktivistas.

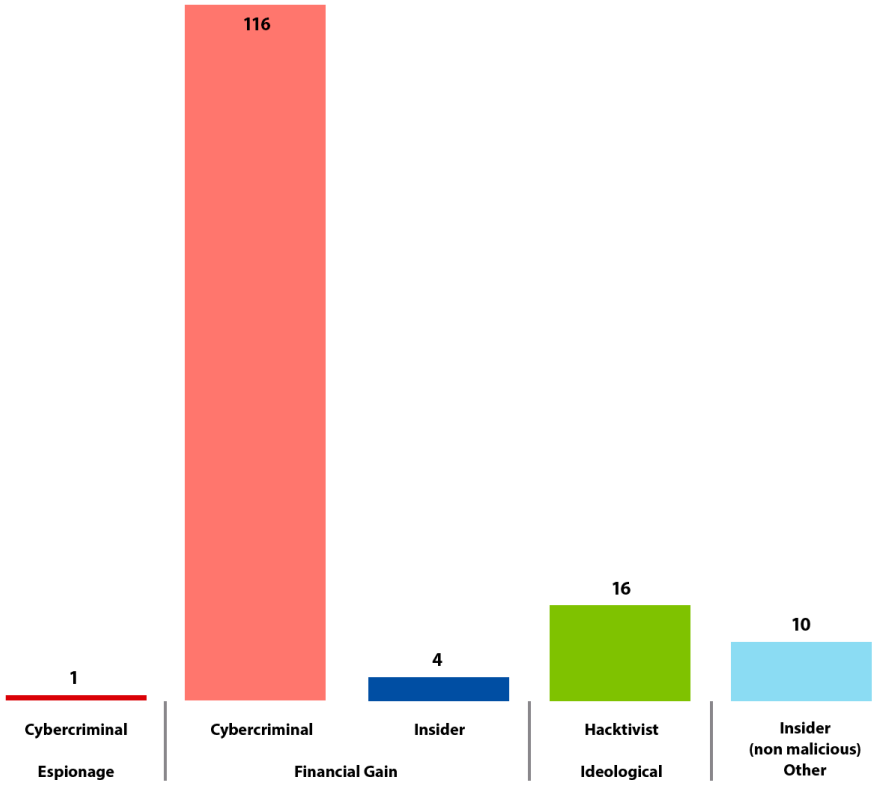
- El principal motivo de los ciberdelincuentes es el beneficio económico, a menudo robando datos o pidiendo rescates. El informe concluye que esta es la principal motivación de los autores de las amenazas (83%). Los hackers de alquiler venden sus servicios a personas que no tienen las habilidades o capacidades para hacerlo. Los denominados actores patrocinados por el Estado atacan a las organizaciones para comprometer, robar, cambiar o destruir información.

- Los hacktivistas tienen motivaciones políticas, sociales o ideológicas y atacan a las organizaciones para hacerse publicidad o para provocar un cambio. La motivación ideológica fue el segundo motor de los ataques, con un 10%.

- Además, aparece la figura del actor interno tanto con intención maliciosa (empleado actual o antiguo) como con intención no maliciosa, errores humanos, configuraciones erróneas y malas prácticas de seguridad). El 7% de los incidentes fueron involuntarios

8 ENISA Threat Landscape 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Gráfico 2.
Actores de las amenazas y motivación.



Al analizar los actores más destacados que afectan al panorama sanitario europeo y su motivación, surgen dos categorías principales de actores: el primero y predominante es el de los ciberdelincuentes, en particular los implicados en actividades de ransomware, cuya principal motivación es el beneficio económico. El segundo grupo está formado por organizaciones hacktivistas motivadas por razones ideológicas, cuyo objetivo es llevar a cabo ataques de denegación de servicio (DoS) contra organizaciones y autoridades sanitarias.

V. Impacto.

El informe de ENISA que analizamos considera que los efectos de las ciberamenazas en el sector sanitario de la UE afectan a:

a Las historias clínicas electrónicas. Los datos de los pacientes incluyen el historial médico del paciente y otros datos sanitarios que constituyen información sensible y crucial para tratar adecuadamente a un paciente. Son datos personales y protegido jurídicamente que afectan al diagnóstico y el tratamiento.

b Sistemas y servicios de información que son clave en la atención al paciente. Relativos a registros y citas, seguimiento de la evolución del paciente, servicios de laboratorio, acceso a servicios de farmacia, dispositivos inteligentes para la atención sanitaria, sistemas automatizados para el seguimiento de la atención a ancianos, botones de emergencia, etc.

c Los sistemas y redes informáticos no médicos. Incluyen el resto de los sistemas informáticos que no se utilizan para la atención al paciente, por ejemplo, la página web de la institución, los sistemas administrativos, etc.

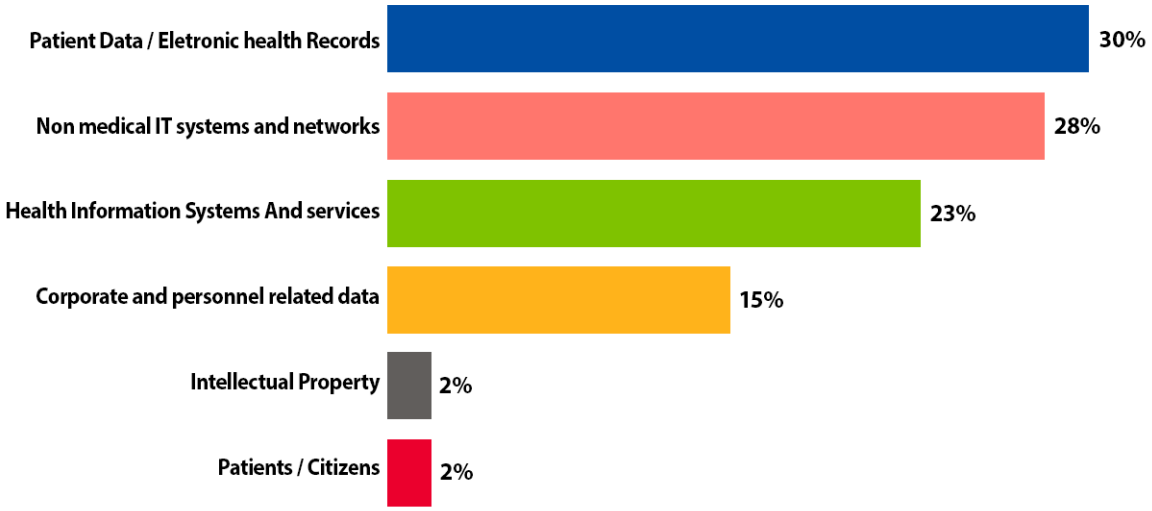
d Los datos corporativos y relacionados con el personal son información que no está relacionada con la atención al paciente. Esta información es confidencial pero no está asociada a la asistencia sanitaria.

e La propiedad intelectual sanitaria. Incluye informa-

ción relacionada con patentes, aspectos no funcionales de un dispositivo médico o teorías y resultados asociados a la investigación científica.

Los datos de los pacientes, incluidas las historias clínicas electrónicas, fueron los más atacados en 63 casos identificados (30%). Los datos de los pacientes se consideran una mercancía, ya que pueden utilizarse para robar la identidad de una persona y cometer fraude o para extorsión y chantaje. Los historiales de los pacientes no sólo incluyen datos personales (por ejemplo, nombres completos, números de la seguridad social, información de identificación, direcciones de correo electrónico, información sobre tarjetas de crédito), sino también información relacionada con la salud, como información demográfica, historiales médicos, resultados de pruebas o de laboratorio, estados de salud mental, etc. Estos datos pueden venderse después en la dark web y otros foros de acceso especial. En un estudio reciente se puede encontrar una muestra de este tipo de historiales que se venden, con precios que varían en función de lo completo que sea el historial médico robado[9].

Los sistemas y redes informáticos no médicos se vieron afectados en 55 incidentes (28%), los sistemas de información sanitaria en 48 (23%) y los datos corporativos y relacionados con el personal en 31 incidentes (15%).



VI. Recomendaciones.

En general, los distintos informes de la Agencia Europea de Ciberseguridad han dado más luz sobre los tipos de ciberincidentes, los actores y sus motivaciones, los activos afectados, las víctimas y los impactos potenciales en el sector sanitario europeo. Esto puede proporcionar información valiosa para la gestión de riesgos tanto a las autoridades gubernamentales sanitarias europeas como a los profesionales de la ciberseguridad del sector. Sobre la base de toda esta información, la Agencia Europea propone las siguientes recomendaciones a los Estados miembros, al sector sanitario y a sus profesionales:

A **Retos para el sector sanitario**. Uno de los principales motivos de preocupación son las vulnerabilidades de los dispositivos médicos y su posible efecto en la seguridad y la privacidad de los pacientes. La Prospectiva de Amenazas a la Ciberseguridad de ENISA para 2030 incluye, como mayor amenaza futura, los ataques dirigidos a personas utilizando los datos recogidos en dispositivos inteligentes y equipos médicos.[10]

B **Recomendaciones para los profesionales sanitarios**. Las organizaciones sanitarias y sus profesionales debieran seguir prácticas de ciberhigiene como las siguientes:

9 Recorded Future, The business of Fraud: Sales of PII and PHI, by Insinkt Group, February 17, 2021, p. 10. https://go.recordedfuture.com/hubfs/reports/cta-2022-0217.pdf

10 ENISA Foresight Cybersecurity Threats for 2030, March 2023. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

- Las copias de seguridad cifradas fuera de línea de datos de misión crítica con información confidencial (datos en reposo) pueden mitigar los riesgos de fuga de datos.

- Los programas de sensibilización y formación de los profesionales sanitarios pueden contribuir a mitigar los ataques de ingeniería social y a mejorar las prácticas de seguridad entre los usuarios.

- Deben seguirse buenas prácticas en los métodos de autenticación para el acceso remoto.

- Crear, mantener y ejercitar planes básicos de respuesta a incidentes cibernéticos para garantizar que la atención al paciente no se vea afectada. Estos pueden incluir planes de contingencia en cada departamento o servicio, mejora de los canales de comunicación, pero también cuidado de los profesionales sanitarios y de su bienestar mental y físico.

- El compromiso de la alta dirección del sector sanitario es clave, especialmente ahora que la directiva NIS2 introduce responsabilidades para la alta dirección.

C **Recomendaciones a los Estados**. En Europa, las organizaciones sanitarias deben cumplir diversos reglamentos y normas, como las Buenas Prácticas Clínicas,[11] la normativa sobre productos sanitarios (MDR)[12] y el Reglamento General de Protección de Datos (RGPD). El incumplimiento de estas normas puede acarrear graves consecuencias, como acciones legales, sanciones.
El sector sanitario maneja información muy sensible y personal. Por tanto, el cumplimiento de esta normativa es crucial para proteger la intimidad de los pacientes, mantener la confianza y garantizar su seguridad y bienestar. La notificación de incidentes y sus posibles repercusiones puede suscitar preocupación por los fallos en el cumplimiento de la normativa y, por tanto, revelar posibles incumplimientos.
En el caso de las entidades públicas que dependen de la financiación pública vía presupuestos de Estado y del apoyo de los contribuyentes, los incidentes suelen tener un impacto más público. Aunque puede haber implicaciones financieras, éstas suelen ser menos directas en comparación con las entidades privadas. En cambio, para el sector privado, los incidentes pueden tener un impacto directo en la confianza de los clientes y en la imagen de la organización sanitaria. Aunque no sea deseable y pueda abrir aún más riesgos legales en el futuro, es una realidad que debemos tener en cuenta a la hora de emprender el control y fiscalización de incidentes.

VII. Propuesta de una fiscalización informática como instrumento de control público.

Los informes recientes de ENISA insisten en la necesidad de implantar prácticas de ciberhigiene, planes de contingencia y mecanismos de verificación continua en el sector sanitario europeo. Estas recomendaciones, sin embargo, requieren un marco de fiscalización que asegure su efectiva aplicación en las organizaciones sanitarias, evitando que se conviertan en meras declaraciones de principios.

En este contexto, la fiscalización informática debe configurarse como un instrumento de apoyo a los órganos de control interno y externo de las Administraciones Públicas, ampliando el alcance del control tradicional hacia la evaluación de la seguridad digital y la protección de los datos de salud.

En este sentido, la fiscalización informática puede aportar un **apoyo técnico especializado** en tres líneas de actuación coherentes con las directrices de ENISA:

1. **Verificación preventiva**: mediante auditorías informáticas periódicas que identifiquen vulnerabilidades en los sistemas sanitarios, evaluando tanto la suficiencia de las medidas de seguridad implantadas como la preparación de los planes de respuesta a incidentes.

2. **Evaluación del cumplimiento normativo**: comprobando la aplicación efectiva de la Directiva

11 Directiva 2001/20/CE del Parlamento Europeo y del Consejo, de 4 de abril de 2001, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros sobre la aplicación de las buenas prácticas clínicas en la realización de ensayos clínicos sobre medicamentos de uso humano; Directiva 2005/28/CE de la Comisión, de 8 de abril de 2005, por la que se establecen los principios y las directrices detalladas de las buenas prácticas clínicas respecto a los medicamentos en investigación de uso humano, así como los requisitos para autorizar la fabricación o importación de dichos productos; Reglamento (UE) n °536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014 , sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE Texto pertinente a efectos del EEE;

12 Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, relativo a los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) no 178/2002 y el Reglamento (CE) no 1223/2009 y se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo.

NIS2, el RGPD y las guías técnicas de ENISA, a través de indicadores objetivos que midan la madurez digital y la resiliencia de las organizaciones sanitarias.

3. **Refuerzo de la rendición de cuentas**: generando información independiente, verificable y comparable que permita fundamentar los informes de fiscalización, detectar deficiencias recurrentes y proponer recomendaciones de mejora estructural.

De este modo, la fiscalización informática no se limita a una función sancionadora, sino que se convierte en un **instrumento de apoyo y prevención**, que fortalece la capacidad de supervisión de los órganos de control público, aporta mayor transparencia al sector sanitario y contribuye a garantizar la protección efectiva de los derechos fundamentales vinculados a los datos de salud.

Bibliografía.

- Directiva 2001/20/CE del Parlamento Europeo y del Consejo, de 4 de abril de 2001, relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros sobre la aplicación de las buenas prácticas clínicas en la realización de ensayos clínicos sobre medicamentos de uso humano.

- Directiva 2005/28/CE de la Comisión, de 8 de abril de 2005, por la que se establecen los principios y las directrices detalladas de las buenas prácticas clínicas respecto a los medicamentos en investigación de uso humano, así como los requisitos para autorizar la fabricación o importación de dichos productos.

- ENISA: Threat landscape: health sector (January 2021 to March 2023) July 2023. ISBN 978-92-9204-638-5 DOI 10.2824/163953 TP-04-23-546-EN-N;

- Threat Landscape 2022, November 2022.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

- Cybersecurity Threat Landscape Methodology, July 2022.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology;

- Threat Landscape 2021.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021;

- Threat Landscape for Ransomware Attacks, July 2022.
https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks;

- Cybersecurity Healthcare Week, May 2023.
https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/boostyourcybervitals; NIS Investments 2022, November 2022.

- https://www.enisa.europa.eu/publications/nis-inv.

- https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/alaris-infusion-central-recoverable-password-vulnerabilit-yestments-2022;

- Foresight Cybersecurity Threats for 2030, March 2023. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030.

- https://govern.cat/salapremsa/notes-premsa/488382/ciberatac-al-clinic-afecta-seva-activitat-assistencial-habitual.

- https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/sanidad-las-islas-baleares-sufre-ciberataque.

- Jareño Butron, M. y Arratibel Arrondo, J.A.: "Recomendaciones de la Agencia Europea de Ciberseguridad ante incidentes de seguridad en el sector sanitario." Revista Auditoría Pública, nº. 83, 2024, págs. 115-137.

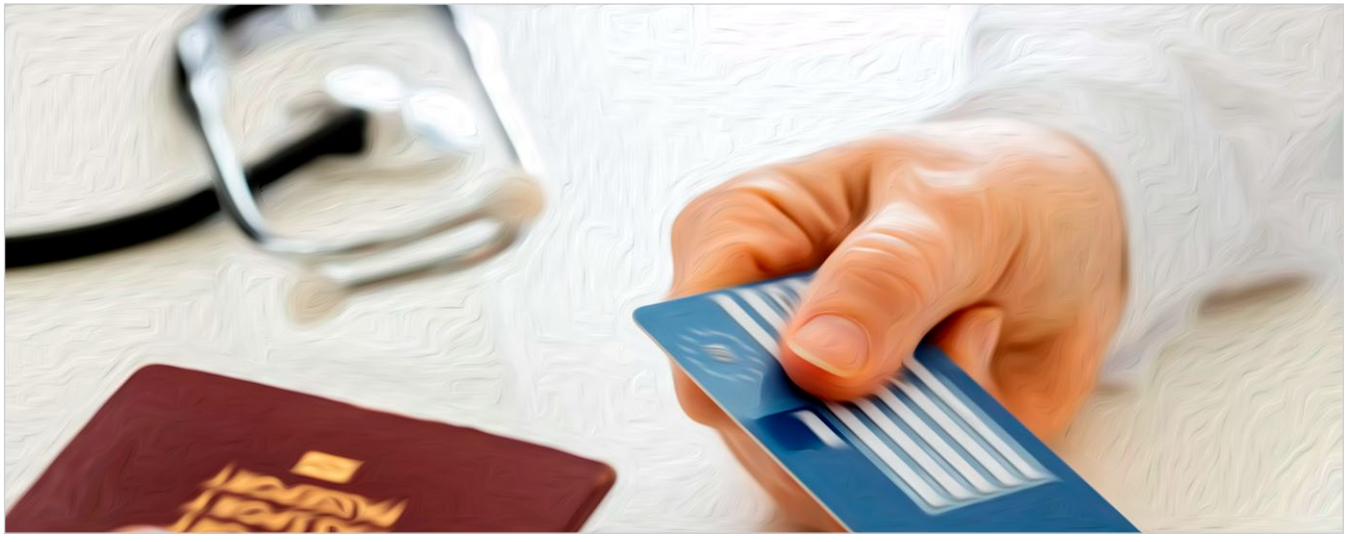
- "Técnicas para el control del tratamiento masivo de datos personales en el sector público sanitario." Revista Auditoría Pública nº 81 enero - junio 2023. Páginas: 180-195;

- "Bases del modelo de respuesta europeo a incidentes de ciberseguridad informática en el sector sanitario." Diario La Ley, ISSN 1989-6913, N.º 10223, 2023;

- "La ciberseguridad como protección del derecho a los datos personales relativos a la salud" en revista noticias jurídica publicado el 3-01-2023 (sección de conocimiento de artículos doctrinales).

- Ponemon Institute, The Impact of Ransomware on Patient Safety and the Value of Cybersecurity Benchmarking, January 2023.
https://www.censinet.com/impact-of-ransomware-on-patient-safety-and-value-of-cybersecurity-benchmarking/

- Recorded Future, The business of Fraud: Sales of PII and PHI, by Insinkt Group, February 17, 2021, p. 10.
https://go.recordedfuture.com/hubfs/reports/cta-2022-0217.pdf

- Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, relativo a los productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) no 178/2002 y el Reglamento (CE) no 1223/2009 y se derogan las Directivas 90/385/CEE y 93/42/CEE del Consejo.

- Reglamento (UE) n °536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE.