La ciberseguridad en un entorno sensible: inmersión en el sector sanitario

LIBRO BLANCO



STORMSHIELD

Los ciberdelincuentes no se detienen ante nada. Frente a la importancia vital del ámbito sanitario, no dudan en aprovecharse de las fragilidades provocadas por la crisis sanitaria o los fallos generados por la transformación digital del sector. Tanto en Francia como a escala internacional, los centros hospitalarios, las farmacias, los laboratorios y otras estructuras de atención sanitaria se enfrentan a oleadas incesantes de ciberataques en un contexto de gran vulnerabilidad informática.

En el ámbito sanitario, en 2021 se declararon el doble de incidentes que en 2020[1]. ¿Cómo se explica esta escalada sin precedentes? Las respuestas son tan variadas como las vulnerabilidades de los establecimientos, a lo que hay que añadir desde hace poco el perfil inédito de algunos objetivos. De hecho, son ahora los actores del sector sanitario los que afrontan esta amenaza.

Los datos sensibles que se transfieren en el ámbito sanitario son motivo de gran preocupación, porque aunque su atractivo para los ciberdelincuentes no deja lugar a dudas, su gestión despierta numerosos debates, sobre todo en el contexto actual de estructuración de un marco normativo europeo.

El objetivo de este libro blanco es permitir a los responsables informáticos, así como a todo el ecosistema de subcontratistas y proveedores del sector sanitario conocer en detalle el estado actual de la cuestión de la ciberseguridad en los establecimientos sanitarios.

Para ello, en las siguientes páginas tratamos de descrifrar los problemas de este sector, presentamos un inventario operativo de posibles soluciones y planteamos algunas proyecciones sobre el futuro de la seguridad informática en este ámbito.

04 — Colaboradores

01. La ciberseguridad en el sector sanitario: ¿por qué es tan frágil?

08 — *Infografía: un repaso a nivel internacional de los ciberataques en los establecimientos sanitarios*
10 — Limitaciones materiales importantes: un parque informático único en su especie
14 — Transformación digital en el sector sanitario: una aceleración tardía que debe mantenerse
16 — El caso particular de los datos sanitarios
17 — *Entrevista a Charles Blanc-Rolin: ¿cuál es la relación entre el acceso a los datos, la sanidad y la protección?*

02. Anatomía de una amenaza polimórfica con múltiples puntos de entrada

22 — ¿Cómo penetran los ciberdelincuentes en los sistemas de información de los establecimientos anitarios?
26 — Todo el itinerario de la atención sanitaria en el punto de mira
28 — Esto no es un ciberataque

03. ¿Qué remedios pueden garantizar la seguridad del sector sanitario?

32 — ¿Qué medidas existen para proteger las infraestructuras sanitarias?
37 — *¿Qué obligaciones normativas tienen los establecimientos sanitarios?*
38 — Una toma de conciencia y unos esfuerzos apoyados por la acción pública
40 — *Entrevista cruzada: ¿el reglamento europeo sobre los datos sanitarios está a la altura de los retos que se plantean?*

04. ¿Qué nos deparará el futuro?

46 — La continuidad de la atención médica a escala europea
48 — Medicina preventiva, supervisión del hospital a través de los datos: las promesas (y los retos) de la aplicación del Big Data a la medicina
50 — Una colaboración que forjar
52 — *Entrevista a Jacky Grisey: El futuro de la ciberseguridad en el sector sanitario*

Colaboradores

CHARLES BLANC-ROLIN

RESPONSABLE DE PROYECTO DE SEGURIDAD DIGITAL EN E-SALUD PAYS DE LA LOIRE (FRANCIA)

«Alguna vez ya he tenido que aplicar soluciones de bloqueo físico de puertos USB junto con el o la responsable biosanitario. Así se evita que alguien utilice, por ejemplo, un ecógrafo para cargar su smartphone...».

PÁGINA 31

¿Cuál es la relación entre el acceso a los datos, la sanidad y la protección?

PÁGINA 17

JACQUES LABIDURIE

CISO, CHU DE LIMOGES

«Los actores industriales deben recibir formación sobre ciberseguridad, porque muchos siguen abordando la informática igual que hace 30 años. En el plan de estudios de medicina debe incluirse también la seguridad informática, no solo la protección de datos como ahora».

PÁGINA 34

JACK GRISEY

SECURITY OPERATIONS MANAGER PARA SANIDAD DE ADVENS

«Los ciberataques importantes que se han producido desde hace unos años han puesto de manifiesto la deuda técnica y organizativa de los sistemas de información de los establecimientos sanitarios. Se ha tomado conciencia incluso en las más altas esferas del Estado».

PÁGINA 42

El futuro de la ciberseguridad en el sector sanitario

PÁGINA 52



CORALIE ACHARD-TORTUL

DPO (DATA PROTECTION OFFICER), CHU (CENTRO HOSPITALARIO UNIVERSITARIO) DE LIMOGES (FRANCIA)

«Es importante situar nuestras acciones de sensibilización en su contexto. Una reunión previa con el jefe de área permite, por ejemplo, comprender cómo funciona y recopilar ejemplos reales, como el hecho de dejar su tarjeta puesta durante las distintas actividades radiográficas... ».

PÁGINA 35

JEAN-SYLVAIN CHAVANNE

RSSI (RESPONSABLE SEGURIDAD INFORMÁTICA), CHU (CENTRO HOSPITALARIO UNIVERSITARIO) DE BREST (FRANCIA)

«Una factura falsa, una solicitud maliciosa de renovación de una contraseña, una reclamación de un paciente imaginario... las campañas de phishing que interceptamos son cada vez más sofisticadas. Algunas incluso han llegado a usurpar la identidad del hospital universitario (CHU, por sus siglas en francés) de Brest.».

PÁGINA 23

La vista puesta en los dispositivos médicos conectados

PÁGINA 13

STÉPHANE PRÉVOST

PRODUCT MARKETING MANAGER EN STORMSHIELD

«Corregir una vulnerabilidad crítica en un componente expuesto en Internet no garantiza la protección frente a un ataque anterior. También hay que analizar los registros para comprobar si se ha aprovechado dicha vulnerabilidad y, en caso de duda, renovar todas las cuentas».

PÁGINA 34

RAYNA STAMBOLIYSKA

EXPERTA EN DIPLOMACIA DIGITAL, ESPECIALISTA EN CIBERSEGURIDAD Y MIEMBRO INDEPENDIENTE DEL GRUPO DE TRABAJO SOBRE AMENAZAS EMERGENTES Y FUTURAS DE LA AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA)

«Los textos de la Ley de servicios digitales y la Ley de mercados digitales, que abordan el tema de forma transversal y sistémica, se basan en los distintos textos, como el RGPD, la directiva NIS o la Ley de datos. Tienen como fin favorecer la innovación, proteger a los ciudadanos europeos y asentar la autoridad estratégica de la Unión Europea».

PÁGINA 37

¿El reglamento europeo sobre los datos sanitarios está a la altura de los retos que se plantean?

PÁGINA 41

DAMIAN KLIMAS

SOCIO DE DOTLAW Y OBSERVADOR DE LA RED EHEALTH NETWORK

«La adopción del Espacio Europeo de Datos Sanitarios (EEDS) acelerará el desarrollo de MiSalud@EU. Eso significa que, de aquí a 2025, los establecimientos sanitarios de todos los Estados miembros y Noruega tendrán un acceso fácil y seguro a las alergias, recetas y antecedentes médicos de cualquier paciente, en su idioma, aunque resida en otro país europeo ».

PÁGINA 47

¿El reglamento europeo sobre los datos sanitarios está a la altura de los retos que se plantean?

PÁGINA 41



01.

La ciberseguridad en el sector sanitario: ¿por qué es tan frágil?

¿Cómo se explica que los centros hospitalarios, las clínicas, las farmacias y los laboratorios sean tan vulnerables a los ciber riesgos? Desde la arquitectura de los sistemas de información sanitaria hasta sus componentes, pasando por los nuevos usos del mundo de la medicina, los motivos son por desgracia muy variados.

Un repaso a nivel internacional de los ciberataques en los establecimientos sanitarios



Centro médico presbiteriano de Hollywood
2016 — ESTADOS UNIDOS

Hospitales de Baton Rouge General, Jack Huston Memorial y Southwest Health[2]
2022 — ESTADOS UNIDOS

Healthcare Service Executive
2021 — IRLANDA

Sistema sanitario de la provincia de Terranova y Labrador[3]
2021— CANADÁ

Hospital infantil de Boston
2014 — ESTADOS UNIDOS

Ministerio de Sanidad
2021 — BRASIL

Organizaciones sanitarias
2020 — REINO UNIDO

National Health Service
2017 — REINO UNIDO

Centro Hospitalario Universitario de Ile-de-France AP-HP
2020 — FRANCIA

Centro Hospitalario SurFrancilien de Corbeil Essonne
2022 — FRANCIA

Sistema francés de Seguros
2022 — FRANCIA

Sistema sanitario[4]
2022 — DINAMARCA

Hospital Universitario de Düsseldorf (UKD)
2020— ALEMANIA

Cadena logística de vacunas contra la COVID[5]
2020— ALEMANIA

Sitio web de referencia dedicado a la salud
2019 — LA INDIA

Hospital de Osaka
2022 — JAPÓN

Grupo de establecimientos sanitarios SingHealth
2018 — SINGAPUR

Centro Hospitalario d'Issoudun
2019 — FRANCIA

Mayorista de una farmacia en Rouen
2020 — FRANCIA

Centros sanitarios
2022— ESPAÑA

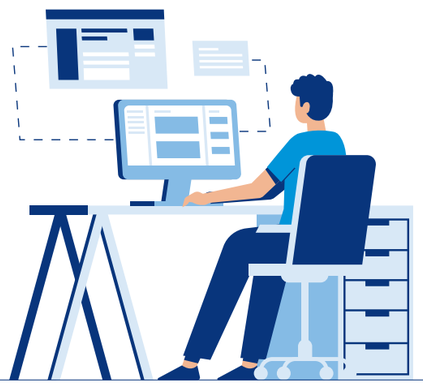
Grupo hospitalario Life Healthcare
2020 — SUDÁFRICA

Hospital de Dharmais y Harapan Kita
2017 — INDONESIA

Aseguradora australiana
2022 — AUSTRALIA

1.1 Limitaciones materiales importantes: un parque informático único en su especie

La red informática constituye una parte crítica del funcionamiento de un hospital. Actúa como una auténtica correa de transmisión con la red operativa y el exterior, pero debe tener en cuenta un parque informático particular y unas problemáticas inherentes al sector sanitario.



OBSOLESCENCIA, CONVERGENCIA DE LOS SI, PERMEABILIDAD DE LAS REDES: PROBLEMÁTICAS COMUNES

Al igual que otros sectores, en particular industriales, el sector sanitario está sujeto a la obsolescencia programada. Así, en los establecimientos sanitarios no es raro enfrentarse a unos parques cuyos programas informáticos no han cambiado desde hace 20 años. Esta larga vida útil, debida a la amortización del material médico, hace que estas versiones de sistemas no reciban mantenimiento y queden obsoletas, como es el caso de Windows XP, lo que fragiliza la seguridad de estos entornos.

Una vulnerabilidad reforzada por la permeabilidad de las redes, al igual que la convergencia de los SI en los grupos hospitalarios territoriales (GHT) en Francia. Como están interconectados de una forma no segura, aumentan el riesgo de propagación de los ciberataques.

Por último, el telemantenimiento, generalizado desde hace tiempo en los hospitales por las intervenciones a distancia de los fabricantes de productos médicos, editores o integradores de aplicaciones, presenta también un riesgo, ya que los accesos son más o menos seguros.

LA GESTIÓN SENSIBLE DE LAS INSTALACIONES HOSPITALARIAS

Si hablamos de ciberseguridad, enseguida pensamos en los sistemas de información. Sin embargo, hoy en día es necesario abordar la cuestión de una forma más amplia por la creciente interconexión entre redes informáticas y redes operativas.

Así, el perímetro abarca también las infraestructuras técnicas (gestión técnica centralizada [GTC] y gestión técnica de instalaciones [GTI]). Estas últimas permiten gestionar la seguridad contra incendios, los accesos, la videovigilancia, la gestión energética e incluso la calidad del aire interior de las instalaciones hospitalarias.

«Aun basándose en el marco general de seguridad (RGS)[6], todavía resulta difícil hacer que los gigantes de la industria biomédica apliquen los requisitos mínimos de seguridad en sus protocolos de telemantenimiento, por ejemplo. En muchos casos, parece todavía muy difícil reforzar la seguridad a este nivel ».

CHARLES BLANC-ROLIN — RESPONSABLE DE PROYECTO DE SEGURIDAD DIGITAL EN E-SALUD PAYS DE LA LOIRE

Estos distintos sistemas operativos, formados por autómatas de marcas y generaciones heterogéneas, demasiado a menudo siguen estando conectados con la red informática de una forma no segura y a veces pasan desapercibidos para los responsables de seguridad de los sistemas de información. Del mismo modo, a menudo se descuida la infraestructura telefónica del establecimiento sanitario. Sin embargo, si se dejaran fuera de servicio los teléfonos IP de un hospital por un ataque distribuido de denegación de servicio (DDoS, por sus siglas en inglés), las consecuencias serían desastrosas.

Este problema es aún más complejo en la medida en que una misma estructura gestiona a veces distintas instalaciones repartidas por el territorio.

DESTACADO

EL ESCENARIO DE UN CIBERATAQUE

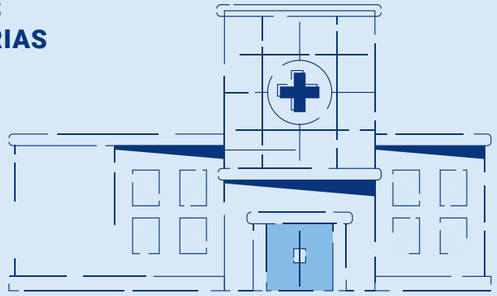
→ Descubra un escenario concreto de un ciberataque dirigido a la seguridad contra incendios de un establecimiento hospitalario. —

NOTA

LA CALIDAD DEL AIRE

es una cuestión de comodidad de las habitaciones de los pacientes, pero resulta vital en los quirófanos.

LA GESTIÓN SENSIBLE DE LAS INSTALACIONES HOSPITALARIAS



- Comunicación con otros servicios de urgencia
- Integración del sistema
- Validación del sistema
- Sistemas comerciales y administrativos
- Servicios a los pacientes
- Gestión energética
- Calefacción, ventilación y aire acondicionado
- Protección del perímetro
- Estructuración y gestión de cables
- Comunicaciones por voz y datos
- Convergencia IP
- Servicios y mantenimiento
- Televisión por antena
- Vídeo de información pública/carteles
- Servicios de muy baja tensión
- Sonorización y anuncios vocales
- Iluminación
- Detección y alarma contra incendios
- Control de los accesos
- Gestión de los ascensores y de las escaleras mecánicas
- Gestión de la localización de los pacientes/bienes/flujos de trabajo clínico
- Seguridad/televisión en circuito cerrado y videovigilancia digital

LA PROTECCIÓN DE LOS EQUIPOS BIOMÉDICOS EN EL PUNTO DE MIRA

Utilizados en radiodiagnóstico médico o incluso en biología, muchos de los equipos biomédicos están conectados al sistema de información (SI).

Eso es lo que permite, por ejemplo, a algunos cirujanos, contar con la ayuda en directo de un o una compañero/a en la otra punta del mundo a través de una cámara conectada.

Además de mejorar la atención de los pacientes, este Internet de las cosas aplicado a la medicina (IoMT, por sus siglas en inglés) contribuye al diagnóstico y mejora la colaboración entre profesionales sanitarios. Incluso ofrece una respuesta parcial a la problemática de los desiertos médicos en el caso de la telemedicina. No obstante, representa un riesgo para la seguridad del hospital.

Estos dispositivos, que rara vez son un objetivo directo, a menudo sufren daños colaterales por los ciberataques. Su debilidad radica en que están conectados a la red sin incorporar la seguridad necesaria a pesar de estar en contacto directo con los pacientes.

Diseñados por unos fabricantes industriales cuya cultura cibernética es limitada, a menudo constituyen posibles fuentes de infección.

ACTUALIDAD

UNA CONTRASEÑA FUERTE

→ En octubre de 2022 se reveló una vulnerabilidad en un equipo de laboratorio médico utilizado para la detección del cáncer de cuello uterino. La culpa fue de los datos de identificación con una fuerte codificación en el equipo.

20.000

CIFRA CLAVE

EQUIPOS BIOMÉDICOS

Se trata del número de equipos biomédicos repartidos por el hospital universitario (CHU, por sus siglas en francés) de Brest.

«Los establecimientos sanitarios no siempre conocen el sistema operativo en el que se basan estos dispositivos, a menudo vulnerable y obsoleto, ni el software, ni las bibliotecas incorporadas. En estas condiciones, resulta difícil reaccionar cuando se publican vulnerabilidades».

CHARLES BLANC-ROLIN — RESPONSABLE DE PROYECTO DE SEGURIDAD DIGITAL EN E-SALUD PAYS DE LA LOIRE

UN SECTOR BAJO PRESIÓN

La ciberseguridad en el sector sanitario también acusa la escasez generalizada de medios del sector. En los últimos años, el Gobierno francés ha ofrecido financiación, pero ésta solo se destina a inversiones y no a mantenimiento. La seguridad informática en la atención médica también achaca una falta de recursos y expertos dedicados. —

«Hoy en día, concentramos nuestros recursos humanos en la seguridad informática en la parte de proyecto: no contamos con ningún recurso operativo a pesar de que se creó un puesto en febrero».

JACQUES LABIDURIE — CISO, CHU DE LIMOGES

ACTUALIDAD

EL ATAQUE QUE COLMÓ EL VASO

Tras el ataque contra el Centro Hospitalario Sud-Francilien[7] en Corbeil-Essonnes (Francia) a finales de agosto de 2022, el Gobierno francés inyectó 20 millones de euros en la Agencia Nacional francesa de Seguridad de los Sistemas de Información (ANSSI) para reforzar su apoyo a los hospitales.

LA VISTA PUESTA EN LOS DISPOSITIVOS MÉDICOS CONECTADOS

CON **JEAN-SYLVAIN CHAVANNE** — RSSI, CHU DE BREST

→ El marcado CE médico. Esta marca de conformidad que se otorga a los productos sanitarios representa un reto de seguridad importante. De hecho, cualquier modificación estructural pondría en peligro el marcado, lo que impide realizar las actualizaciones y los parches de seguridad necesarios en estos objetos o máquinas de uso sanitario.

Esta situación expone a los productos sanitarios en particular a las vulnerabilidades de tipo Log4Shell y obliga a recurrir a soluciones de protección perimétrica (compartimentación de redes, elementos de supervisión, etc.).

Este enfoque requiere unas competencias precisas que los equipos informáticos no siempre dominan. Por lo tanto, existe un verdadero desafío de formación sobre ciberseguridad y colaboración entre los departamentos informáticos, de CISO y de biomedicina.

De lo contrario, seguirán dándose situaciones críticas, como en los equipos de radioterapia aún infectados por el gusano informático Conficker en 2022 debido a una versión obsoleta de Windows. —

1.2 Transformación digital en el sector sanitario: una aceleración tardía que debe mantenerse

En los últimos años, es innegable la transición del sector sanitario hacia la ciber salud. El sector se encuentra en plena reorganización. Está adoptando nuevos usos que se han puesto a prueba en el delicado contexto de la pandemia de la COVID-19.



EL AUGE DE LA TELEMEDICINA Y LA TELEVIGILANCIA

El recurso cada vez más habitual a la telemedicina y la televigilancia, sobre todo en las hospitalizaciones a domicilio, amplía la superficie de ataque potencial de los establecimientos sanitarios. De hecho, cuando un paciente cuenta con asistencia respiratoria en casa, su respirador puede convertirse en un nuevo punto de entrada al sistema de información del hospital.

EXTERNALIZACIÓN DE LOS SERVICIOS

El servicio más emblemático de estos usos es, sin duda, la externalización de la concertación de citas a través de plataformas en línea, como Doctolib, que da lugar a una buena cantidad de preguntas y polémicas, sobre todo a propósito de la seguridad de los datos intercambiados.

«El recurso masivo a servicios digitales externalizados, a menudo menos protegidos, es una práctica muy extendida que los atacantes aprovechan».

ANSSI — 2020[8]

FALLOS HUMANOS: EL DESCONOCIMIENTO DE LOS CIBER RIESGOS

Además, está el factor humano, porque la transformación digital en el ámbito de la salud influye en los empleados de los establecimientos sanitarios y no todos los empleados tienen los mismos reflejos de higiene digital... Tal como indica la ANSSI en su guía de higiene digital: «*Cada usuario constituye de por sí un eslabón de la cadena de los sistemas de información. En este sentido, en cuanto llega a la entidad, debe ser informado de los retos de seguridad, las reglas que deben respetarse y los comportamientos adecuados en materia de seguridad de los sistemas de información, a través de acciones de sensibilización y formación*».

Una fragilidad reforzada por la práctica del «Bring Your Own Device» (BYOD): algunos médicos, cuyo tiempo se divide entre su consulta privada y el hospital, utilizan material no proporcionado por este último, que no siempre cumple las normas de seguridad informática. —

26 de enero de 2022

FECHA CLAVE

EL 26 DE ENERO DE 2022 EN FRANCIA

En esa fecha, la Alta Autoridad Sanitaria publicó los cuatro primeros marcos de televigilancia médica para las siguientes patologías: diabetes, insuficiencia cardíaca crónica, insuficiencia renal crónica e insuficiencia respiratoria crónica.

Llegarán más trabajos para enriquecer esta base, con el fin de desplegar la televigilancia de forma duradera y segura. —

1.3 El caso particular de los datos sanitarios

El sector sanitario está en el punto de mira de los ciberdelincuentes por la gran cantidad de datos que maneja, sensibles y vitales por naturaleza. ¿Cuáles son estos datos y cuáles son los retos que conllevan?



¿CUÁL ES LA RELACIÓN ENTRE EL ACCESO A LOS DATOS, LA SANIDAD Y LA PROTECCIÓN?

ENTREVISTA

CHARLES BLANC-ROLIN — RESPONSABLE DE PROYECTO DE SEGURIDAD DIGITAL EN E-SALUD PAYS DE LA LOIRE



«Los cirujanos preferirán volver a una medicina de guerra: esto implica renunciar a los datos antes que fiarse de unos datos que puedan ser erróneos o parciales».

¿Cómo definiría un dato sanitario?

C.BR — El término designa cualquier dato relativo a la salud del paciente, tanto si se trata de un informe de una operación como del presupuesto de una intervención médica o incluso de una cita con un profesional sanitario.

¿Cómo está ligado el acceso a estos datos sanitarios a la seguridad de los pacientes?

C.BR — La cuestión de los datos sensibles a menudo se aborda desde el prisma de la **confidencialidad**. El público general teme que se divulguen los números de sus tarjetas bancarias, pero no es consciente de las consecuencias que puede tener el robo de su número de seguridad social. Pues bien, en el caso de los datos sanitarios, más que en ningún otro caso, las consecuencias son graves. La **integridad** de los datos es una cuestión de seguridad: si se cambia una posología o se elimina la mención de una alergia, la vida del paciente puede estar en juego. La **disponibilidad** también es muy importante: por ejemplo, los cirujanos necesitan imágenes para operar.

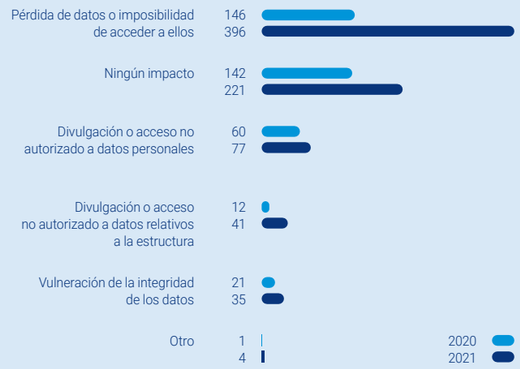
¿Por qué es crítica la confianza en los datos en el ámbito sanitario?

C.BR — Retomando el ejemplo de los cirujanos, preferirán volver a una medicina de guerra: esto implica renunciar a los datos antes que fiarse de unos datos que puedan ser erróneos o parciales.

¿La inaccesibilidad de los datos es frecuente en el sector sanitario?

C.BR — Según el CERT-Santé, el organismo francés competente en materia de ciberseguridad en el ámbito sanitario, esto era así para «todos o parte de los datos de las aplicaciones de la estructura» en la mitad de los incidentes señalados en 2021. —

DISTRIBUCIÓN DE LOS INCIDENTES DE SEGURIDAD POR TIPO DE IMPACTO EN LOS DATOS



Fuente: Observatorio de las denuncias de incidentes de seguridad de los sistemas de información en el sector sanitario (2021)

UN NÚMERO CRECIENTE DE DATOS QUE DEBEN PROTEGERSE

Otro parámetro que debe tenerse en cuenta es que el volumen de datos generados por los establecimientos sanitarios no ha dejado de crecer en los últimos años.

La digitalización está claramente presente en el día a día de los especialistas con el despliegue de los servicios digitales de base como «Mon espace santé» en Francia. Este espacio, disponible desde principios de 2022, permite a todos los franceses y francesas encontrar sus documentos sanitarios (recetas, resultados de analíticas, etc.), indicar datos personales sobre sus antecedentes familiares y hablar de forma segura con los profesionales sanitarios.

La tecnología digital también forma parte ahora del proceso de trabajo del personal médico, tal como ilustra la multiplicación de herramientas de ayuda al diagnóstico como Psychaclic[9] o la obligación que existe en Francia desde el 1 de marzo de 2022 de expedir los certificados de defunción por vía electrónica.

Unas bases de datos cada vez más nutridas cuya gestión y mantenimiento para garantizar su conformidad serán cada vez más complejos, entre las obligaciones de conservación y el derecho a la supresión[10] que establece el RGPD...

UNA MINA (DE ORO) DE INFORMACIÓN

Si bien los datos sanitarios pueden ser motivo de actos maliciosos destinados a desestabilizar las operaciones de un hospital o perjudicar a una persona en concreto, a los ciberdelincuentes les encantan porque su venta es muy lucrativa. Ejemplo de junio de 2022: se pusieron a la venta 1000 millones de datos personales chinos, que incluían información médica, por la cantidad de 10 bitcoins (200.000 dólares)[11].

CIFRA CLAVE

Entre 50 y 250 euros

HISTORIA CLÍNICA
Es el precio de reventa de una sola historia clínica[12]

x30

CIFRA CLAVE

EL VOLUMEN TOTAL DE DATOS SANITARIOS DIGITALES
En 2016, la Agencia Nacional francesa de apoyo al rendimiento de los establecimientos sanitarios y médico-sociales (ANAP, por sus siglas en francés) indicó que el volumen total de datos sanitarios digitales se duplicaba cada 73 días, por lo que, desde entonces, se habría multiplicado por 30.

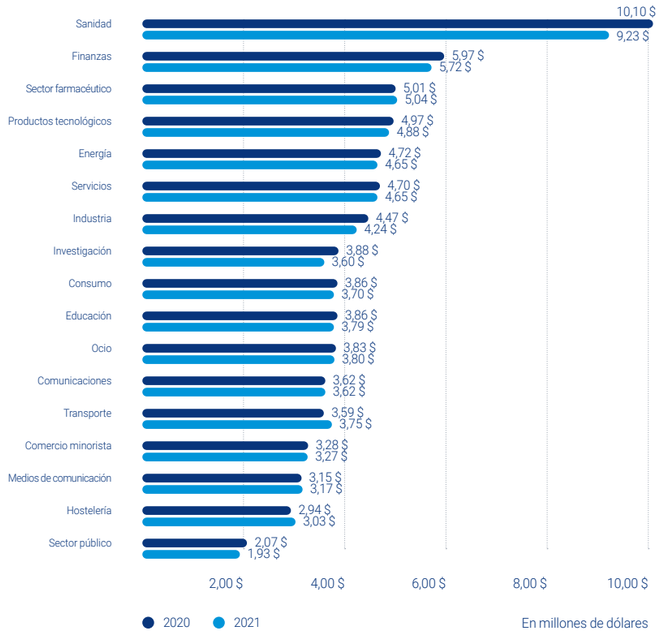
Los datos sanitarios constituyen, por tanto, un recurso muy preciado que interesa también a otros actores como los gigantes tecnológicos. La web de investigación The Markup[13] reveló en junio de 2022 que los establecimientos sanitarios estadounidenses transmitían información sensible (nombre del médico, palabras clave buscadas o patologías) sobre sus pacientes en Facebook mediante su uso del «Píxel de Meta».

UNAS FUGAS QUE SALEN CARAS

Estas cuestiones, cada vez más mediatizadas sensibiliza poco a poco a la opinión pública. La reputación de las empresas víctimas también se ve afectada, como en el caso de Shields, un grupo estadounidense de diagnóstico por imagen y cirugía ambulatoria que sufrió un robo de datos que afectó a casi 2 millones de personas.

Sin embargo, el coste correspondiente no es nada desdeñable. Un informe de IBM[14] estima que el coste medio de una violación de datos en el caso de una estructura sanitaria supera los 10 millones de dólares. —

EL COSTE MEDIO DE UNA FUGA DE DATOS POR MERCADO VERTICAL, DOMINADO POR LA SANIDAD



1,5 M€

CIFRA CLAVE

MULTA
1,5 millones de euros. Es el importe de la multa que se impuso a la empresa Dedalus Biologie por una brecha de seguridad «que dio lugar a la fuga de datos médicos de casi 500 000 personas» (Comisión Nacional francesa de Informática y Libertades, CNIL).

PARA PROFUNDIZAR

CINCO WEBINARS ESPECÍFICOS

→ Descubra nuestra serie de de 5 webinarss[15] para profundizar en la cuestión de la hipersensibilidad de los entornos hospitalarios frente a los ciberataques.



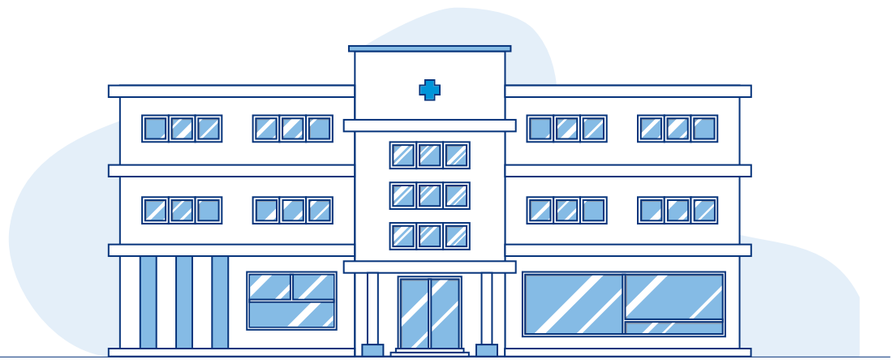
02.

Anatomía de una amenaza polimórfica con múltiples puntos de entrada

¿Por qué vectores penetra la ciber amenaza en los establecimientos sanitarios? ¿Cuáles son los distintos tipos de ataques que sufren? ¿Son siempre incidentes dirigidos? A los ciberdelincuentes no les falta el ingenio para atacar el sector sanitario, pero, en ocasiones, el incidente de seguridad se debe a un fallo y no a un ciberataque. Ahora bien, sus consecuencias son igual de desastrosas.

2.1 ¿Cómo penetran los ciberdelincuentes en los sistemas de información de los establecimientos sanitarios?

Lamentablemente, son muchos los puntos de entrada de las ciber amenazas en las estructuras sanitarias. Se pueden agrupar en cuatro vectores.



1. HUMANO

Los ciberataques utilizan o se dirigen a una o varias personas (médicos, enfermeros, agentes, administradores e incluso los propios pacientes).

En 2020, un mayorista de Rouen (Francia), proveedor de las farmacias de la región, hizo un pedido por valor de 6,6 millones de euros en geles y mascarillas a una empresa que resultó ser fantasma. Un ejemplo dramático del «fraude del CEO»[16] en el contexto delicado de la pandemia de la COVID-19.

2. SOFTWARE

Los ciberataques de software agrupan todos los ataques que explotan una debilidad, una brecha o la obsolescencia de un programa instalado en un equipo informático o un instrumento médico informatizado.

En 2020, una polémica puso de manifiesto un cierto número de brechas de seguridad en una solución del grupo Dedalus, especializado en software sanitario. Una de ellas permitía acceder a las incidencias abiertas por los hospitales y laboratorios de clientes de la empresa, en las que podían encontrarse identificadores y contraseñas de tele-administración.

3. RED

Como su propio nombre indica, un ciberataque a la red corresponde a todos los ciberataques que transitan por la red del hospital.

Los servicios de Assistance Publique – Hôpitaux de Paris (AP-HP) sufrieron en 2020 un ataque a la red por denegación de servicio (DDoS) en dos de sus direcciones web. Como resultado de dicho ataque, los empleados sufrieron problemas de acceso al correo electrónico y las aplicaciones.

4. FÍSICO

Los ciberataques físicos agrupan los ataques destinados específicamente a la dimensión material de un equipo médico, informático u operativo.

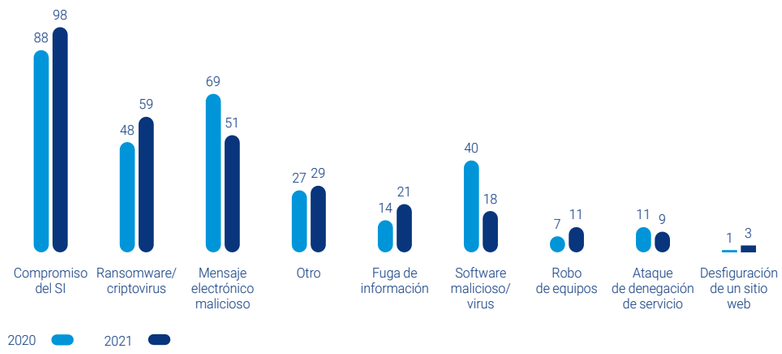
En 2019, unos investigadores israelíes simularon un ataque de tipo «*man-in-the-middle*» introduciendo un Raspberry Pi en un hospital. Así, pudieron interceptar los datos de diagnóstico médico por imagen transmitidos a través del protocolo DICOM y demostrar que podían alterarse.

Con independencia del vector de ataque elegido por el ciberdelincuente, la «carga viral» más habitual en el sector de la sanidad es actualmente el ransomware. Sin embargo, las estructuras sanitarias también están muy expuestas a los ataques de denegación del servicio distribuido y al robo de datos. —

«Una factura falsa, una solicitud maliciosa de renovación de una contraseña, una reclamación de un paciente imaginario, las campañas de phishing que interceptamos son cada vez más sofisticadas. Algunas incluso han llegado a usurpar la identidad del hospital universitario (CHU) de Brest. No obstante, el aumento más flagrante se refiere a los initial access brokers (IAB). Estos corredores de accesos iniciales están especializados en buscar identificadores de usuarios para revenderlos».

JEAN-SYLVAIN CHAVANNE —
CISO, CHU DE BREST

NÚMERO DE INCIDENTES POR TIPO DE ORIGEN



Fuente: informe IBM Security, Cost of Data Breach (2022)



2.2 Todo el itinerario de la atención sanitaria en el punto de mira

Hospitales y clínicas representan el primer objetivo de los ciberataques en el ámbito sanitario. Sin embargo, no son los únicos. Laboratorios, proveedores e incluso pacientes están también en el punto de mira de los ciberdelincuentes.



Varios establecimientos hospitalarios estadounidenses ya pagaron el precio en 2022 (Baton Rouge General en Louisiana, Jack Huston Memorial en Phoenix y el Southwest Health Center en Wisconsin), como también en Francia (Vitry-le-François, Saint-Dizier, Charleville-Mézières, Corbeil-Essonnes) y España (Barcelona).

Sin embargo, los ataques también apuntan a los laboratorios; por los datos médico-administrativos de los que se apoderan en programas de biología médica de tipo Mega Bus[18].

Últimamente los ciberdelincuentes han ampliado aún más su abanico de objetivos. Por una parte, ahora atacan a los distintos proveedores, que pueden abrirles las puertas virtuales de los sistemas de información de los establecimientos hospitalarios. Y, por otra, ya no dudan en atacar a los propios pacientes, que se convierten en víctimas de chantaje tras el robo de sus datos sanitarios o personales. —

CUANDO LOS CIBERDELINCUENTES ATACAN A LOS PACIENTES

→ En 2020, los pacientes de una veintena de centros de psicoterapia finlandeses, gestionados por la empresa Vastaamo, se llevaron la desagradable sorpresa de recibir una petición de rescate de 500 euros en Bitcoin bajo la amenaza de la difusión de los datos recopilados durante sus sesiones. Un caso de doble extorsión[19] que generó miles de reclamaciones a las autoridades. —

CUANDO LOS CIBERDELINCUENTES ATACAN A LA CADENA LOGÍSTICA

→ En 2020, algunos proveedores especializados en la cadena de frío de las vacunas contra la COVID-19 fueron el objetivo de una campaña de phishing. El objetivo era recuperar información sensible sobre su transporte y distribución. De acuerdo con los investigadores de ciberseguridad de IBM, la campaña que tiene las características de un ataque a nivel estatal. . —

2.3 Esto no es un ciberataque

Aunque, obviamente hay que adoptar todas las medidas necesarias para protegerse de los ciberataques, no hay que olvidar que incluso los incidentes de origen no malicioso pueden tener consecuencias graves en el sistema sanitario.



En un entorno hospitalario vulnerable y frágil, un incidente informático puede dar lugar a un incidente de seguridad. Como en junio 2022 en el hospital universitario (CHU, por sus siglas en francés) de Nantes, donde una avería importante, provocada por el antivirus instalado, afectó a todos los equipos de trabajo con Windows 7, incluidos los equipos biomédicos, que quedaron inutilizables. —

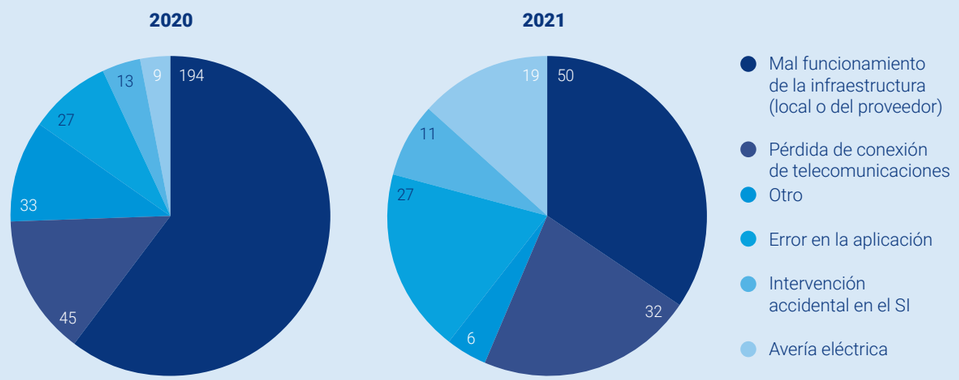
48 %

CIFRA CLAVE

NO MALICIOSO

El 48 % de las denuncias al Observatoire CERT-Santé[20] no son de origen malicioso

DISTRIBUCIÓN DE LOS INCIDENTES DE ORIGEN NO MALICIOSO



Fuente: Observatorio de las denuncias de incidentes de seguridad de los sistemas de información en el sector sanitario (2021)



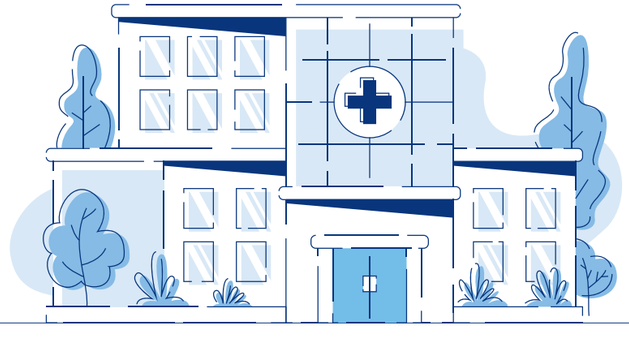
03.

¿Qué remedios pueden garantizar la seguridad del sector sanitario?

¿Cómo protegerse de los ciberataques? ¿Qué dice la legislación actual al respecto? ¿Qué ayuda pueden proporcionar las autoridades a este nivel? El proceso puede ser complejo, pero es vital para protegerse bien.

3.1 ¿Qué medidas existen para proteger las infraestructuras sanitarias?

Las infraestructuras de los establecimientos sanitarios son vitales por naturaleza. El rendimiento y la disponibilidad de las redes informáticas de nuestros sistemas sanitarios son importantísimos, sobre todo cuando la vida de los pacientes depende a menudo de la información que permiten intercambiar.



ETAPA 1: AUDITORÍA Y ANÁLISIS DE RIESGOS

La primera medida de cualquier iniciativa de ciberprotección debe referirse al conocimiento de los sistemas. En esta fase, el objetivo es identificar los activos más sensibles para reducir la superficie de ataque definiendo una política de seguridad.

«Este mapeo permite identificar y clasificar los componentes de los sistemas de información y de los sistemas operativos de las estructuras sanitarias según distintos criterios, como la obsolescencia o la criticidad».

STÉPHANE PRÉVOST — PRODUCT MARKETING MANAGER EN STORMSHIELD

ETAPA 2: DESPLIEGUE DE SOLUCIONES DE SEGURIDAD ADAPTADAS

Estos medios, proporcionados por equipos como los que ofrece Stormshield, cubren distintos perímetros.

Protección de las redes

Algunas de las funcionalidades que deben reunirse para proteger las redes informáticas hospitalarias son:

- La segmentación de la red,
- El control de los accesos, la gestión del telemantenimiento y otros accesos a distancia,
- La protección de las comunicaciones,
- La autenticación en dos factores
- El filtrado por el usuario
- La protección de los protocolos de comunicación de los equipos biomédicos (prevención de la intrusión IPS OT) .

Protección de los puestos de trabajo

Para beneficiarse de una protección reforzada de sus terminales, los establecimientos sanitarios deben asegurarse de implantar:

- La autenticación en dos factores,
- La prevención de la intrusión en los puestos de trabajo (HIPS) mediante el análisis de comportamiento,
- La gestión de los periféricos externos (hasta la implantación de estaciones blancas).

«Alguna vez ya he tenido que aplicar soluciones de bloqueo físico de puertos USB junto con el o la responsable de biomedicina. Así se evita que alguien utilice, por ejemplo, un ecógrafo para cargar su smartphone y ponga en peligro el dispositivo».

CHARLES BLANC-ROLIN — RESPONSABLE DE PROYECTO DE SEGURIDAD DIGITAL EN E-SALUD PAYS DE LA LOIRE

LA SEUDONIMIZACIÓN O LA REVERSIBILIDAD DEL ANONIMATO

CON **JEAN-SYLVAIN CHAVANNE** — CISO; CHU DE BREST

→ *«Una de las particularidades del ámbito sanitario es que algunos datos sensibles no pueden anonimizarse por completo: por ejemplo, un centro sanitario puede tener que dirigirse a posteriori a un paciente que haya seguido un tratamiento específico. Por eso, los datos del paciente se dividen en dos bases de datos para permitir su reidentificación si fuera necesario». —*

También es necesario aplicar una política de contraseñas suficientemente robusta[21] para evitar ser víctima de acciones maliciosas a través de Internet.

Por último, la mejora del seguimiento de las acciones correctivas es indispensable para aumentar el nivel de seguridad de los puestos de trabajo en las estructuras sanitarios. Para ello, hay que asegurarse de vigilar los componentes expuestos y actualizarlos cuando se proporcione una acción correctiva, abordando de forma prioritaria las vulnerabilidades críticas. El drama del ciberataque al hospital de Düsseldorf se podía haber evitado: siete meses antes se había proporcionado un parche de la vulnerabilidad explotada.

Protección de datos

Si bien la primera medida a este nivel es evitar el envío de las historias de los pacientes por correo electrónico sin cifrar, existen otras medidas necesarias. Es necesario garantizar:

- Una historia clínica cifrada con distintas claves de acceso,
- El cifrado de extremo a extremo de la información, en particular cuando se extrae del SI para transmitirla a otro hospital (en los casos de atención médica coordinada, por ejemplo),
- Un proceso de anonimización y seudonimización para un tratamiento eficaz de los datos.



ETAPA 3: VERIFICACIÓN Y MEJORA CONTINUA

La siguiente etapa consiste en controlar la conformidad y comprobar las divergencias respecto a la política de seguridad. Para eso es conveniente:

- analizar regularmente los registros de los equipos perimétricos,
- realizar auditorías de seguridad o test de penetración,
- relanzar una fase de planificación para aplicar acciones correctivas.

«El interés de las estructuras sanitarias por un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) gestionado confirma el atractivo de la combinación de recursos habida cuenta de las dificultades de contratación en estos puestos (escasez de perfiles, financiación, etc.)».

JACKY GRISEY — SECURITY OPERATIONS MANAGER PARA SANIDAD DE ADVENS

«Corregir una vulnerabilidad crítica en un componente expuesto en Internet no garantiza la protección frente a un ataque anterior. También hay que analizar los registros para comprobar si se ha aprovechado otro componente de dicha vulnerabilidad y, en caso de duda, renovar todas las cuentas».

STÉPHANE PRÉVOST — PRODUCT MARKETING MANAGER EN STORMSHIELD

INICIAR UN PROCESO DE SENSIBILIZACIÓN Y FORMACIÓN

La sensibilización es imprescindible para poder aumentar el nivel de protección de los establecimientos sanitarios. Estas campañas deben dirigirse en primer lugar a los profesionales del sector como aquí en Centre-Val de Loire[22] con el desarrollo de **plataformas de sensibilización y formación** para establecimientos sanitarios y médico-sociales. Sin embargo, estas acciones de comunicación y sensibilización deben dirigirse también a los pacientes y a los fabricantes de productos sanitarios con un tono adaptado a cada grupo de destinatarios.

«Los actores industriales deben recibir formación sobre ciberseguridad, porque muchos siguen abordando la informática igual que hace 30 años. En el plan de estudios de medicina debe incluirse también la seguridad informática, no solo la protección de datos como ahora».

JACQUES LABIDURIE — CISO, CHU DE LIMOGES

Algunos actores no dudan en ir más lejos en la responsabilización de los usuarios. Ahora, el centro hospitalario de Calais registra las sesiones en sus servidores[23], que se consideran críticos. Esta nueva política se aplica incluso a sus proveedores, el 40 % de los cuales hacen lo mismo.

No obstante, en este sector sometido ya a una gran presión es imprescindible **que la ciberseguridad sea coherente con las prácticas sectoriales:** por ejemplo, la solicitud reiterada de contraseñas de 12 caracteres en situaciones de urgencia no son adecuadas. —

¿CÓMO SE PUEDEN PROTEGER LOS DISPOSITIVOS MÉDICOS SIN PONER EN RIESGO SU MARCADO CE?

→ La principal solución de seguridad de red consiste en compartimentar las redes y aislarlas del resto del SI a través de una microsegmentación. Así, cuando surge una necesidad de cambio de flujo, hay que tratar de contar con un filtrado muy fino y prever, si es posible, la detección de anomalías en estos mismos flujos a través de una sonda IDS, por ejemplo. —

«Es importante situar nuestras acciones de sensibilización en su contexto. Una reunión previa con el jefe de área permite, por ejemplo, comprender cómo funciona y recopilar ejemplos reales, como el hecho de dejar su tarjeta puesta durante las distintas actividades radiográficas. Los departamentos administrativos, de compras y de investigación clínica tienen todos un vocabulario específico que debemos dominar para ser eficaces».

CORALIE ACHARD-TORTUL — DPO, CHU DE LIMOGES

CIBERPROTEGER LAS ESTRUCTURAS SANITARIAS CON STORMSHIELD

CIBERSEGURIDAD EN EL ÁMBITO SANITARIO

→ Stormshield participa en el establecimiento de una ciberseguridad de confianza a escala europea. Todas las gamas de productos se enmarcan en un proceso continuo de cualificación y certificación de seguridad ante las autoridades europeas competentes.

STORMSHIELD NETWORK SECURITY PARA LA PROTECCIÓN DE REDES

Dado que la disponibilidad de los servicios es clave en este universo, la gama de cortafuegos Stormshield Network Security (SNS) garantiza la continuidad y la disponibilidad de los servicios gracias a su segmentación de red, su funcionalidad de bypass o incluso su sistema de prevención de intrusiones. Asimismo, para proteger los datos de los pacientes durante las conversaciones, estos cortafuegos protegen los accesos a distancia de telemantenimiento a través de las redes privadas virtuales (VPN, por sus siglas en inglés).

STORMSHIELD DATA SECURITY PARA LA PROTECCIÓN DE DATOS

La protección de los datos sanitarios se ha convertido en un eje central y vital para los establecimientos sanitarios. Con un cifrado de extremo a extremo, Stormshield Data Security (SDS) preserva la integridad y la confidencialidad de la información sensible. En particular a la hora de extraer datos del sistema de información.

STORMSHIELD ENDPOINT SECURITY PARA LA PROTECCIÓN DE LOS SERVIDORES Y LOS PUESTOS DE TRABAJO

Para respaldar la transformación del sector sanitario y los nuevos usos profesionales, la solución Stormshield Endpoint Security (SES) ofrece una protección autónoma de los terminales, capaces de modificar de manera dinámica los niveles de protección en función de su entorno.

STORMSHIELD LOG SUPERVISOR PARA LA VISIBILIDAD DE LOS EVENTOS DE RED

Gracias a la herramienta Stormshield Log Supervisor (SLS), se puede conocer de un vistazo el estado de la red informática y acceder a los registros de eventos. Una solución idónea para optimizar las labores de investigación y la respuesta a incidentes.

¿QUÉ OBLIGACIONES NORMATIVAS TIENEN LOS ESTABLECIMIENTOS SANITARIOS?



EN ESTADOS UNIDOS

→ Se aplica la Health Insurance Portability and Accountability Act (HIPAA) estadounidense, así como su sección sobre datos personales de índole sanitaria bautizada como ePHI (por las siglas en inglés de «electronic Protected Health Information»).

EN EUROPA

→ La directiva NIS 2 recoge una serie de obligaciones para los operadores de servicios esenciales (OSE) de los que forman parte la mayoría de los establecimientos sanitarios que disponen de un servicio de urgencias médicas. Entre ellas, existe la obligación de declarar los incidentes de seguridad. Como todas las organizaciones de la Unión Europea, también deben cumplir el RGPD.

EN FRANCIA

→ Estos establecimientos sensibles, clasificados a veces como operadores de importancia vital (OIV), están también sujetos al Código francés de salud pública, a la orden interministerial n.º 901 en la PGSSI-S. Desde abril, está disponible el primer documento oponible de esta última, el marco de identificación electrónica[24]. Este impone a los establecimientos y a los editores unas obligaciones sobre la identificación de los pacientes y profesionales para reforzar la seguridad de los accesos. Además, las estructuras sanitarias pueden consultar la guía de buenas prácticas editada por la Agencia Nacional francesa de Seguridad de los Sistemas de Información (ANSSI).

3.2 Una toma de conciencia y unos esfuerzos apoyados por la acción pública

Sin embargo, la vulnerabilidad de los establecimientos sanitarios no es una novedad y preocupa a los profesionales desde hace más de una década. Ya hay iniciativas, tanto a nivel europeo como nacional.



EN EUROPA

Frente a la emergencia de una auténtica economía de los datos, la Unión Europea se encuentra en plena reestructuración con todo un abanico de textos que se están estudiando o que ya se aplican:

- Reglamento General de Protección de Datos personales (RGPD).
- Reglamento relativo a la gobernanza europea de datos (Ley de gobernanza de datos).
- Reglamento relativo a un mercado único de servicios digitales (Ley de servicios digitales).
- Reglamento de mercados digitales.

El proyecto de reglamento sobre el Espacio Europeo de Datos Sanitarios (EEDS)[25] es el primer texto vertical del corpus, es decir, el primer texto que propone un marco de intercambio de datos para un sector concreto. Publicado a principios de mayo de 2022, fue calificado de «*nuevo punto de partida de la política de sanidad digital de la Unión*»[26] por Margaritis Schinás, vicepresidente de la Comisión Europea. —

FECHA CLAVE

Julio de 2016

En julio de 2016, Europa abordó la ciberseguridad a través de la directiva NIS y la identificación de Operadores de Servicios Esenciales (OSE) en el sector sanitario (junto a otros sectores como la energía, el transporte, el agua, la banca o incluso las infraestructuras digitales). El objetivo era proteger sus sistemas de información esenciales.

«Los trabajos como la Ley de servicios digitales y la Ley de mercados digitales, que abordan el tema de forma transversal y sistémica, se enmarcan en la continuidad de los distintos textos, como el RGPD, la directiva NIS o la Ley de datos. Tienen como fin favorecer la innovación, proteger a los ciudadanos europeos y asentar la autoridad estratégica de la Unión Europea».

RAYNA STAMBOLIYSKA — EXPERTA EN DIPLOMACIA DIGITAL, ESPECIALISTA EN CIBERSEGURIDAD Y MIEMBRO INDEPENDIENTE DEL GRUPO DE TRABAJO SOBRE AMENAZAS EMERGENTES Y FUTURAS DE LA ENISA

ENTREVISTA COMÚN

¿EL REGLAMENTO EUROPEO SOBRE LOS DATOS SANITARIOS ESTÁ A LA ALTURA DE LOS RETOS QUE SE PLANTEAN?

Sí, considerablemente

Este texto responde a los retos a los que nos enfrentamos actualmente. Habrá que actualizarlo de aquí a 5 o 10 años para tener en cuenta las nuevas amenazas que surjan con las tecnología de descentralización, la Web 3.0, etc., pero por el momento **se trata de un complemento del RGPD y la directiva NIS que acogemos satisfactoriamente.**

Es un objetivo importante de nuestra historia común, pero parece que es precisamente la pandemia de la COVID-19 la que ha impulsado esta renovación. En este contexto, la red eHealth Network, que reúne a los representantes de los Estados miembros en lo relativo a la tecnología digital aplicada a la sanidad y en el que participo como observador, ha proporcionado un primer ejemplo de cooperación europea: unas herramientas comunes para el desarrollo de aplicaciones móviles de seguimiento del contacto.

La pandemia ha puesto de manifiesto que había que seguir regulando el sector para garantizar realmente la protección de los datos sanitarios. Los dirigentes europeos lo han entendido y este reglamento es prueba de ello. **Propone un esquema de protección del intercambio de información, refuerza las obligaciones de denuncia de incidentes y de interoperabilidad.**

Deberían surgir asimismo diversas normas de certificación (sobre las historias clínicas informatizadas de los pacientes, las aplicaciones de tratamientos, etc.).

Este texto, vinculado también a otras normativas, es uno de los más avanzados: podemos incluso hablar de texto único en lo que respecta a los capítulos sobre el uso primario y secundario de estos datos. Este último abre la vía a un uso para realizar investigaciones con el fin de orientar las políticas de salud pública y mejorar el seguimiento del paciente. —



DAMIAN KLIMAS — SOCIO DE DOTLAW Y OBSERVADOR DE LA RED EHEALTH NETWORK

No, no exactamente

Como marco sectorial, el texto está vinculado con el marco horizontal que plantea la directiva NIS2 en relación con los retos de seguridad. Sin embargo, el artículo 50 proporciona elementos específicos sobre la seguridad de los accesos.

Este texto tiene como fin proponer un marco de intercambio de datos que tendrá un impacto importante en la forma en que se usan los datos en Europa. Sus aspiraciones son considerables: armonizar la noción de utilización secundaria de los datos sanitarios entre los distintos Estados e implantar una infraestructura tecnológica robusta para permitir la valorización de estos datos.



RAYNA STAMBOLIYSKA — EXPERTA EN DIPLOMACIA DIGITAL, ESPECIALISTA EN CIBERSEGURIDAD Y MIEMBRO INDEPENDIENTE DEL GRUPO DE TRABAJO SOBRE AMENAZAS EMERGENTES Y FUTURAS DE LA ENISA

En esta fase, plantea cuestiones ligadas al control de los datos durante este intercambio. **Podemos lamentar la creación de un derecho de acceso incoherente con el definido ya por el RGPD**, que podría dar lugar a situaciones de incertidumbre jurídica. Además, el tema del control por el interesado no está suficientemente tratado: el órgano de gobierno del EEDS no establece, por ejemplo, un representante de los pacientes.

Por último, **la cuestión de la puesta en marcha de este espacio no está clara todavía:** puede llevar a creer que se trata de constituir una enorme base de datos única, cuando, en realidad, el texto prevé interconectar distintas bases descentralizadas.

Esta arquitectura plantea un gran número de preguntas (gobernanza, itinerario de los usuarios, formatos de los datos, procedimientos de recurso, etc.) cuyas respuestas no pueden ni deben ser únicamente tecnológicas. —

IMPORTANTE

→ Este reglamento establece no obstante algunas exigencias técnicas de seguridad sobre cuestiones prácticas de acceso y trazabilidad (ver el artículo 50).

132

CIFRA CLAVE

132 establecimientos franceses participan en el proceso de ciberseguridad («Parcours de cybersécurité») del plan France Relance

CHARLOTTE DRAPEAU — RESPONSABLE DE LA OFICINA DE SALUD Y SOCIEDAD, ANSSI, 2022[29]

A NIVEL NACIONAL

El Gobierno francés presentó en abril de 2019 una hoja de ruta para *acelerar la revolución digital en el sector sanitario*[27] en el marco de un plano más amplio, bautizado como *«Ma Santé 2022»*. Esta publicación fue seguida de la de una doctrina técnica[28]. Revisada anualmente, plantea un marco de referencia y propone una trayectoria a todos los actores de la ciber sanidad en Francia.

La faceta digital del «Ségur de la santé» se inscribe en este marco de referencia y pretende acelerar el proceso de transformación. A través de esta figura, el Ministerio de Solidaridad y Sanidad ha puesto a disposición 2000 millones de euros con el objetivo de acompañar la transición digital de los establecimientos sanitarios y médico-sociales, modernizar los sistemas de información existentes y reforzar la interoperabilidad, la convergencia y la seguridad. Este presupuesto incluye 350 millones de euros especialmente dedicados a la ciberseguridad de estas estructuras.

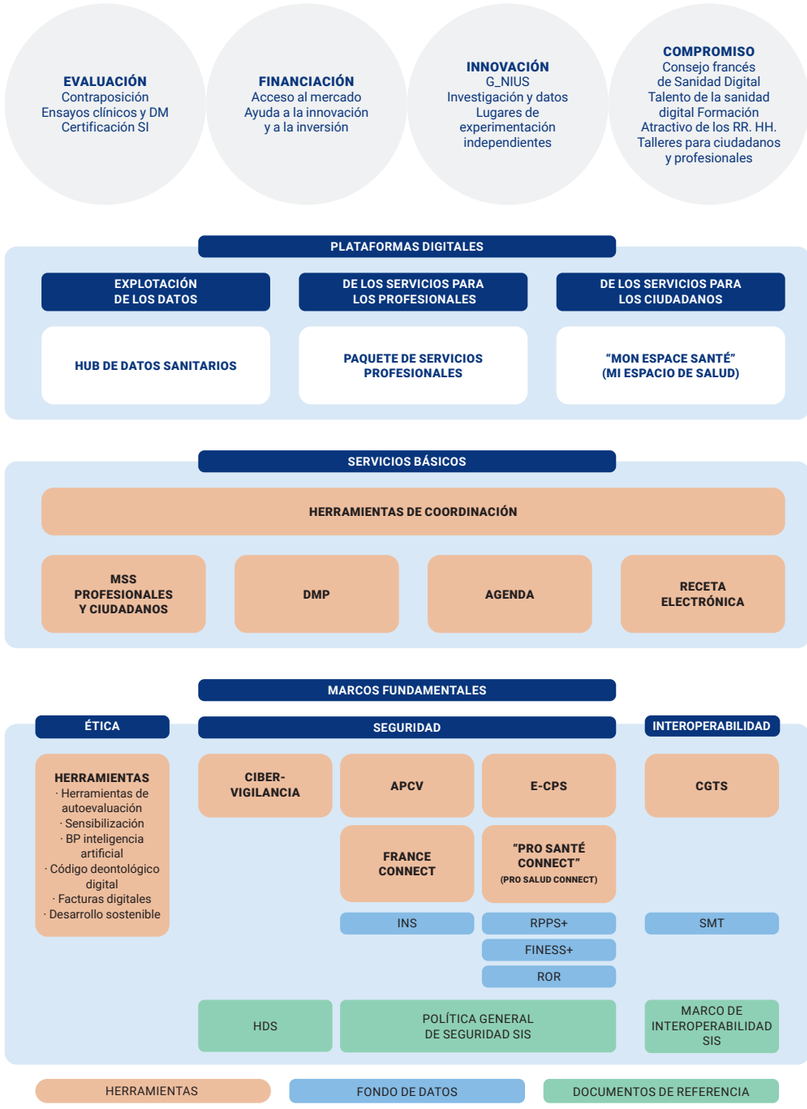
Por otra parte, la ANSSI recibió una dotación de 136 millones de euros para el plan France Relance a fin de reforzar la ciberseguridad del Estado. De esta cantidad, 25 millones se destinarán a la ciberprotección de los establecimientos sanitarios a través de la realización de auditorías en el marco del proceso de ciberseguridad. —

«Los ciberataques importantes que se han producido desde hace unos años han puesto de manifiesto la deuda técnica y organizativa de los sistemas de información de los establecimientos sanitarios. Se ha tomado conciencia incluso en las más altas esferas del Estado ».

JACKY GRISEY — SECURITY OPERATIONS MANAGER PARA SANIDAD DE ADVENS

LOS COMPONENTES DEL MARCO DE REFERENCIA PROPORCIONADO POR EL ESTADO FRANCÉS

Este esquema resume los componentes del marco de referencia de la ciber sanidad en Francia, que debe leerse de forma ascendente: primero, los marcos fundamentales, después los servicios básicos y, por último, las plataformas digitales.



Fuente: Doctrina de la sanidad digital, Ministerio francés de Solidaridad y Sanidad (2021)



04.

¿Qué nos deparará el futuro?

¿Cómo será el sector sanitario en los próximos años?
¿Qué consecuencias tendrá en su seguridad informática?
Un ejercicio de prospectiva que pone de relieve la magnitud de la tarea.

4.1 La continuidad de la atención médica a escala europea

El intercambio de datos sanitarios entre los profesionales del sector, los investigadores y los actores industriales debe permitir a los ciudadanos disfrutar de una mejor atención médica. Esta es la promesa del Espacio Europeo de Datos Sanitarios (EEDS) impulsado por la Comisión Europea. A condición de que la interoperabilidad vaya de la mano de la seguridad.





Si el reglamento sobre el EEDS se aprueba sin grandes cambios, el programa MiSalud@UE (MyHealth@EU) será obligatorio en la Unión Europea y permitirá a todos los ciudadanos disfrutar de la continuidad de su atención médica en todos los Estados miembros. El servicio ya se aplica en Francia a través del portal Sesali.fr desde julio de 2021[30].

La interoperabilidad y la seguridad de los datos deberían seguir siendo los ejes centrales de las políticas sanitarias europeas en los próximos años. —

«La adopción del EEDS acelerará el desarrollo de MiSalud@EU. Eso significa que, de aquí a 2025, los establecimientos sanitarios de todos los Estados miembros y Noruega tendrán un acceso fácil y seguro a las alergias, recetas y antecedentes médicos de cualquier paciente, en su idioma, aunque resida en otro Estado europeo».

DAMIAN KLIMAS — SOCIO DE DOTLAW Y OBSERVADOR DE LA RED EHEALTH NETWORK

4.2 Medicina preventiva, supervisión del hospital a través de los datos: las promesas (y los retos) de la aplicación del Big Data a la medicina

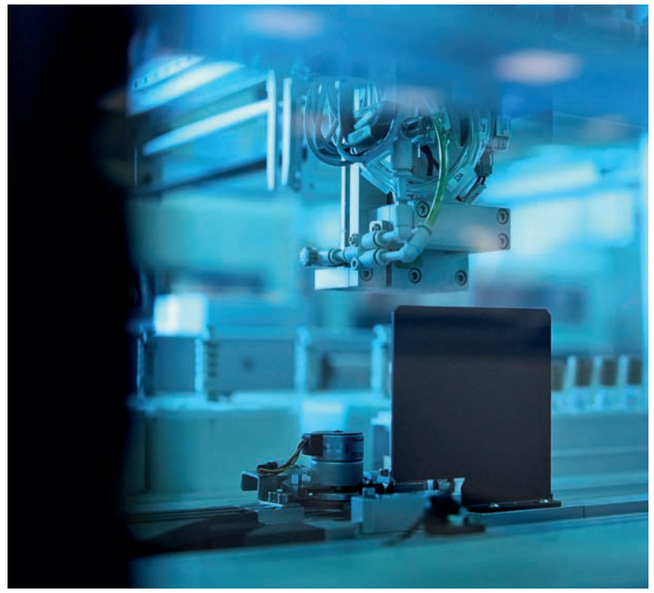
Aunque la recopilación de datos sanitarios parece una tarea relativamente fácil, su tratamiento y análisis son acciones más complejas. Tras la noción de la aplicación del Big Data a la medicina, las promesas de una medicina personalizada y predictiva están sujetas a exigencias de ciberseguridad.



Estas dimensiones serán aún más estratégicas en la medida en que las perspectivas ligadas a la explotación de grandes cantidades de datos son prometedoras. Numerosas empresas se basan en el aprendizaje automático para poner herramientas de diagnóstico a disposición del personal médico. Por ejemplo, la start-up lituana Ligence[31] proporciona un programa informático de análisis de ecocardiografías para los cardiólogos. Estas soluciones deben integrar la cuestión de la ciberseguridad desde su diseño.

«Si queremos detectar las patologías en el futuro más que tratarlas, debemos dominar las cuestiones de la gobernanza de los datos sanitarios y, por lo tanto, también las medidas de seguridad asociadas. Por eso, la misión del RSSI en los establecimientos sanitarios consiste en crear las condiciones necesarias para esta confianza en los SI hospitalarios tanto de los profesionales como de los pacientes».

JEAN-SYLVAIN CHAVANNE — CISO, CHU DE BREST



Sobre las cuestiones de supervisión de las estructuras sanitarias a través de los datos, algunos actores como el Fondo FHF[32] estiman que el PMSI (Programa de Medicalización de los Sistemas de Información), como primera base de datos sobre medicalización nacional, proporciona información suficientemente estructurada para alimentar un algoritmo de minería de procesos. Una operación permitiría en definitiva comparar los datos recabados sobre el terreno, procedentes del PMSIm, con un itinerario ideal del paciente y optimizar la atención médica poco a poco. —

«El margen de progresión es todavía muy importante antes de realizar una supervisión a través de los datos y muchos establecimientos sanitarios todavía están valorando la situación y elaborando una hoja de ruta».

CHARLES BLANC-ROLIN — RESPONSABLE DE PROYECTO DE SEGURIDAD DIGITAL EN E-SALUD PAYS DE LA LOIRE

PARA PROFUNDIZAR

RESPONSABLE DE DATOS
→ Acceder a los datos está bien, pero compartirlos es aún mejor. Aunque el intercambio de datos permite a los investigadores a escala internacional poner en común sus recursos, este proceso debe respetar una normativa muy estricta, destinada a proteger y asegurar los datos relativos a los pacientes, una tarea que justifica la creación de la figura del responsable de datos sanitarios.

4.3 Una colaboración que forjar

Con la integración de la biomedicina y de los sistemas operativos de gestión técnica de instalaciones, la cobertura en materia de SSI de los establecimientos será cada vez mayor, lo que hace imprescindible reunir a todos los actores: informática, SSI y sector biosanitario.



Desarrollar esta cooperación implica conciliar las prioridades y el ritmo de unos y otros: por un lado, el departamento de sistemas de información quiere avanzar rápido y, por otro, los equipos informáticos, que se sienten más o menos responsables de la seguridad (aunque tienen privilegios más altos) o el sector biosanitario no quieren que sus pacientes corran ningún riesgo.

La colaboración también tiene que desarrollarse a nivel ofimático, con una presencia cada vez mayor de tecnologías en la nube. Esta evolución de los usos debe contar con un acompañamiento, ya que su manejo presenta un auténtico desafío.

El sector sanitario tendrá que afrontar nuevos retos asociados a la gobernanza, la cooperación y la técnica para garantizar la seguridad de los pacientes en un entorno cada vez más digitalizado.

«Cuanto más avanzamos por la vía tecnológica, más debemos tener en cuenta la seguridad de los sistemas de información. Si históricamente las relaciones con los equipos especializados han sido a menudo complicadas, los responsables de seguridad de los sistemas de información sanitaria deben esforzarse para hacer comprender a las demás funciones que nuestro reto común es la confianza».

JACQUES LABIDURIE — CISO, CHU DE LIMOGES

«Comprender las implicaciones técnicas y tecnológicas se convierte en una obligación, sobre todo cuando observamos del otro lado del Atlántico la imposibilidad de controlar el destino de los datos sanitarios de las mujeres en un contexto de penalización del aborto. […] Hoy más que nunca, todos y todas debemos contribuir a la construcción de un sistema inteligente y resiliente que respete los derechos y libertades fundamentales».

RAYNA STAMBOLIYSKA — EXPERTA EN DIPLOMACIA DIGITAL, ESPECIALISTA EN CIBERSEGURIDAD Y MIEMBRO INDEPENDIENTE DEL GRUPO DE TRABAJO SOBRE AMENAZAS EMERGENTES Y FUTURAS DE LA ENISA

Unos retos que no deberán eclipsar la misión de servicio público y atención que tradicionalmente desarrolla el sector: habrá que lograr *«recuperar el aspecto humano en la máquina»* tal como pedía la Defensora de los derechos Claire Hédon[33] al micrófono de France Inter en julio de 2022. —

«Solo el futuro nos dirá si el sector sanitario conseguirá circunscribir el ciber riesgo. No obstante, todo apunta a que la digitalización acelerada y las competencias cada vez mayores de los grupos de ransomware no facilitarán la subsanación de su deuda técnica».

JACKY GRISEY — SECURITY OPERATIONS MANAGER PARA SANIDAD DE ADVENS

EL FUTURO DE LA CIBERSEGURIDAD EN EL SECTOR SANITARIO

ENTREVISTA

JACKY GRISEY — SECURITY OPERATIONS MANAGER PARA SANIDAD DE ADVENS



«La puesta en común en el marco de un Servicio de Operaciones de Ciberseguridad (SOC, por sus siglas en inglés) gestionado contribuye a una forma de inteligencia colectiva, beneficiosa y característica del sector sanitario».

Algunas expectativas del sector en materia de ciberseguridad operativa se refieren a la automatización. Utilizamos ya la automatización para el trabajo de nuestros análisis de seguridad, lo que nos permite optimizar los tiempos de detección. Existe un desafío muy importante relativo a la subsanación, con el objetivo de reducir al máximo el tiempo de respuesta. Desde el punto de vista del establecimiento, la primera etapa de la automatización es la delegación de la respuesta al socio en un marco operativo preciso. Después podemos plantear la ejecución automática de respuestas «sencillas»: bloqueo de direcciones IP, creación de listas negras de nombres de dominio de mensajería, cuentas de usuarios, etc., y eso puede requerir un cambio de mentalidad de los equipos informáticos.

Otra evolución futura se refiere al ámbito biomédico, en particular a la gestión de vulnerabilidades y la detección de incidentes por el SOC. Tenemos algunos clientes que han iniciado el desarrollo de sondas específicas, lo cual permite ampliar la superficie de detección. Los actores de los sistemas de información están de acuerdo en una cosa: ¡el dominio es una zona oscura!

En definitiva, solo el futuro nos dirá si el sector sanitario conseguirá circunscribir el ciber riesgo. De momento, toca hacer malabares entre la deuda técnica, la digitalización de las actividades, que está haciéndose a gran velocidad, y la industrialización de los grupos de ciberatacantes. Sin embargo, la puesta en común en el marco de un SOC gestionado, es decir, el hecho de que unos aprovechen lo que se hace para otros (detección de vulnerabilidades, índices de compromiso, reglas de detección o incluso especificidades de integración) contribuye a una forma de inteligencia colectiva, beneficiosa para todos. —

FUENTES Y ANEXOS

[1] CERT Santé
[2] https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise
[3] https://health-trends.co.uk/wi-ga-la-hospitals-confirm-recent-healthcare-cyberattacks/
[4] https://health-trends.co.uk/wi-ga-la-hospitals-confirm-recent-healthcare-cyberattacks/
[5] https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cyberattack-update-march-29-22-1.6401700
[6] lefigaro.fr/secteur/high-tech/covid-19-des-cyberattaques-contre-la-chaine-logistique-des-vaccins-20201203
[7] https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
[8] https://www.usine-digitale.fr/article/le-gouvernement-injecte-20-millions-d-euros-dans-l-anssi-pour-renforcer-son-accompagnement-des-hopitaux.N2036952
[9] https://www.ssi.gouv.fr/actualite/lanssi-et-le-bsi-alertent-sur-le-niveau-de-la-menace-cyber-en-france-et-en-allemagne-dans-le-contexte-de-la-crise-sanitaire/
[10] https://www.psychiaclic.fr/
[11] https://www.dsih.fr/article/4790/effacer-une-donnee-medicale-d-un-patient-vraiment.html
[12] https://www.france24.com/fr/%C3%A9co-tech/20220705-fuite-de-donn%C3%A9es-il-affirme-mettre-en-vente-la-vie-priv%C3%A9e-des-deux-tiers-des-chinois
[13] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites
[14] https://www.ibm.com/security/data-breach
[15] https://www.stormshield.com/fr/webinar-sante-face-aux-cybermenaces/ https://www.dsih.fr/article/4790/effacer-une-donnee-medicale-d-un-patient-vraiment.html
[16] https://www.leparisien.fr/faits-divers/coronavirus-le-milieu-medical-nouvelle-cible-des-arnaques-au-president-01-04-2020-8292336.php
[18] https://www.lemondeinformatique.fr/actualites/lire-dedalus-biologie-ecope-d-une-amende-d-1-5-meteuro-par-la-cnil-86527.html
[19] https://www.lemonde.fr/pixels/article/2020/10/27/la-finlande-secouee-par-le-piratage-de-milliers-de-dossiers-de-patients-en-psychotherapie_6057561_4408996.html [20] https://esante.gouv.fr/sites/default/files/media_entity/documents/mss_ans_rapport_public_observatoire_signalements_issis_2021_vf.pdf
[21] https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/documents-secteur-sante/ACSS_Sensibilisation_s%C3%A9curit%C3%A9_mot_passe.pdf
[22] https://www.esante-centre.fr/portail_pro/services-d-accompagnement/ssi-securite-des-systemes-d-information-131-111.html
[23] https://www.lemagit.fr/etude/Cybersecurite-du-systeme-de-sante-beaucoup-reste-a-faire
[24] https://esante.gouv.fr/sites/default/files/media_entity/documents/webinaires_ie-usagers_2022-05-09_v2.pdf
[25] https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en
[26] https://esante.gouv.fr/actualites/lespace-europeen-des-donnees-de-sante-cest-parti
[27] https://solidarites-sante.gouv.fr/IMG/pdf/190425_dossier_presse_masante2022_ok.pdf
[28] https://esante.gouv.fr/sites/default/files/media_entity/documents/Doctrine_du_numerique_en%20santé_Version%202021_Février%2022_VF.pdf
[29] https://sante-achat.info/performance/charlotte-drapeau-anssi-le-secteur-de-la-sante-est-une-cible-particulierement-vulnerable/
[30] https://sesali.fr/ncpehfr-gui/index.html
[31] https://www.ligence.io
[32] https://www.fondsfhf.org
[33] https://www.francetvinfo.fr/societe/services-publics-il-n-est-pas-possible-d-imposer-a-tout-le-monde-d-avoir-un-smartphone-alerte-la-defenseure-des-droits_5238622.html

LA OPCIÓN EUROPEA EN CIBERSEGURIDAD

WWW.STORMSHIELD.COM

Queda prohibida toda difusión, reproducción o representación, incluso parcial, de este estudio para fines distintos al uso privado en cualquier soporte, lo que podría comprometer la responsabilidad civil y penal de toda persona que no cumpla esta prohibición.
Copyright © 2023 Stormshield

STORMSHIELD