I+S

NÚMERO 159 · ABRIL 2024



ESPECIAL

RETOS Y LÍMITES DEL USO DE DATOS EN SALUD

ACTIVIDADES DE LA SEIS

XXI REUNIÓN DEL FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD

Entidades Asociadas 2024

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Abbott
accenture
AGFA HealthCare
ayesa
aws
BABEL
bahia software
Bosonit
Canon CANON MEDICAL
CGM CompuGroup Medical
COSTAISA
Cynerio Healthcare Cybersecurity
Dedalus HEALTHCARE SYSTEMS GROUP
Deloitte.
dexcom
EVIDEN
Evidenze Knowledge in Health
EY Building a better working world
FUJIFILM Value from Innovation
GE HealthCare
gmv INNOVATING SOLUTIONS
IaaS365
IBM
InterSystems Creative data technology
inetum Positive digital flow
Medikus HEALTH TECH ECOSYSTEM
Microsoft
minsait | sia An Indra company
NOVARTIS
NTT DATA
NUTANIX
N World
oesia grupo
opencloud factory
openline trusted cloud solutions
ORION HEALTH
PLEXUS TECH
PHILIPS
relyens
Roche
sanofi
SAVANA
TECNOLOGÍA Y PERSONAS
TriNetX
T Systems
VIDAL VADEMECUM INTERNACIONAL A VIDAL GROUP COMPANY
werfen

AÑO 2024 NÚMERO 159 **SUMARIO**

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Directora
Zaida Sampedro

Coordinador de Especiales:
Juan Carlos Oliva

Comité Editorial
Luciano Sáez
Jesús Galván
Francisco Martínez del Cerro
Guillermo Vázquez
José Manuel Morales Pastora

Comité de Redacción
Adolfo Muñoz Carrero
Ángel Blanco Rubio
Carlos Gallego Pérez,
Carlos García Codina
Carlos Parra Calderón
Carmen Ferrer
Carmen Recalde
Elvira Alonso Suero
Fernando Báez
Francisco Javier Francisco Verdu
Francisco Sánchez Laguna
Gregorio Gómez
Inmaculada C. Castejón Zamudio
Inmaculada Moro
Javier López Cavero
Javier Turumbay
José Quintela
José Luis Monteagudo
José Manuel Morales Pastora
José María Leal Pozuelo
José Sacristán
Juan Díaz
Juan Fernando Muñoz
Juan Ignacio Coll
Lola Ruiz
Luz Fidalgo
Miguel Ángel Benito Tovar
Santiago Thovar

Colaborador Técnico
Diego Sáez

Información, Publicidad, Suscripciones y Distribución:
CEFIC. C/ Enrique Larreta, 5 Bajo Izda 28036 Madrid
Tlfno: 913 889 478
e-mail: cefic@cefic.es

Producción Editorial:
EDITORIAL MIC
Tel. 902 271 902 · 987 27 27 27
www.editorialmic.com

DL: M-12746-1992
ISSN: 1579-8070

5 **EDITORIAL**

6 **ESPECIAL** RETOS Y LÍMITES DEL USO DE DATOS EN SALUD
6 El compromiso de Akamai con la ciberseguridad del sector sanitario
8 Entornos seguros para los datos de salud
10 Ciberseguridad integrada para la protección del dato sanitario
12 ¿Debe el sector sanitario (pre) ocuparse por la ciberseguridad?
14 La receta ante una epidemia de *ransomware*: seguridad integrada
16 El reto de la protección del dato de salud
18 Capture información sobre el tráfico para monitorear y proteger los entornos de IT sanitarios. Lecciones extraídas de experiencias reales
20 Tecnología digital para la medicina personalizada: biogenética y redes federadas de datos
22 Cartera EUDI: Revolucionando la identidad europea
24 *Malware* y robo de datos: 2023, un año convulso para la ciberseguridad en el sector salud
26 EMMA: Innovación nacional en Ciberseguridad Preventiva– más vale prevenir
27 VPN innovadora: protegiendo de manera preventiva todos los accesos a servicios centrales-usuarios internos y terceros
28 La cuantificación del riesgo ciber como arma del CISO
31 Cumplimiento del ENS mediante el perfil de cumplimiento específico para salud
33 Ciberseguridad y salud conectada: desafíos en cada rincón del sector sanitario
36 Retos del uso secundario de los datos de salud
38 Calidad del dato en la codificación clínica ¿realmente nos importa?
40 Más allá de la consulta: la Ciberseguridad como pilar de la sanidad moderna

43 **ACTIVIDADES DE LA SEIS**
43 XXI Edición del Foro de Seguridad y Protección de Datos de Salud

59 **FOROS Y SECTORES**
59 Foro de Interoperabilidad
60 Foro de Seguridad y Protección de Datos
61 Foro de Salud Conectada
62 Sector de Informática Médica
63 Sector Enfermería
64 Sector Farmacia

66 **AGENDA**

Los artículos revisiones y cartas publicadas en I+S, representan la opinión de los autores y no reflejan la de la Sociedad Española de Informática de la Salud. Queda prohibida la reproducción total o parcial sin citar su procedencia.

ENTIDADES
COLABORADORAS

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

COLEGIO OFICIAL DE FARMACÉUTIOS DE BADAJOZ

CONSEJO GENERAL DE COLEGIOS OFICIALES DE FARMACÉUTICOS

EMERGRAF, S.L. CREACIONES GRÁFICAS

IDCSALUD

OSAKIDETZA - SERVICIO VASCO DE SALUD

SOCIOS TECNOLÓGICOS PRINCIPALES

Abbott
Dedalus
dexcom
FUJITSU
Microsoft
minsait | sia
An Indra company

SOCIOS TECNOLÓGICOS COLABORADORES

FUJIFILM
Value from Innovation
PHILIPS
Roche
salesforce
T-Systems
SIEMENS Healthineers

“Situación y avances de la transformación digital en el sistema sanitario público”

Coincide la publicación de este número de *I+S*, con la difusión pública de los resultados del *ÍNDICE SEIS 2023*. Es necesario agradecer y reconocer, como en todas las ediciones anteriores, el esfuerzo que los directivos de sistemas y tecnologías de la información de todo el Sistema Nacional de Salud realizan, para facilitar los datos que posibilitan que durante doce años, podamos disponer de una información contrastada sobre la situación y los avances de la transformación digital en el sistema sanitario público, facilitando una foto de la realidad, de los medios que se ponen a disposición de las organizaciones para su estrategia digital y los avances en servicios que se van produciendo.

El *ÍNDICE SEIS* se realiza mediante la recogida de información, a través de unos cuestionarios diseñados por el Comité Asesor Institucional de la Sociedad, formado por los directivos de salud digital de las 17 comunidades autónomas y del Ministerio de Sanidad.

Este cuestionario se va actualizando anualmente, incorporando nuevos indicadores según la evolución de los proyectos tecnológicos que se llevan a cabo y eliminando aquellos indicadores que ya han sido superados, pero sin perder la serie histórica de los doce años que este *ÍNDICE SEIS* lleva realizándose.

Una característica que consideramos básica de este trabajo es que mantiene el anonimato de los datos correspondientes a las comunidades de referencia, y esto es así para evitar la comparación nominativa de una comunidad con otra, evitar la utilización critica de estos datos y para garantizar la fiabilidad de la información suministrada. No obstante, los responsables sanitarios de los diferentes servicios de salud pueden comparar su situación con el resto de comunidades autónomas y evaluar sus planteamientos, sus proyectos de transformación digital y los recursos que ponen a disposición para ello.

Este *ÍNDICE* también tiene un importante valor para la industria, ya que les permite conocer la realidad de las inversiones existentes en el sector, sus oportunidades y su posible evolución.

Para la Sociedad Española de Informática de la Salud es una información clave que nos permite, por medio de su análisis, comprobar cómo está evolucionando la transformación digital sanitaria, los recursos disponibles y las barreras que detectamos.

Con esta información preparamos muchas de nuestras iniciativas y propuestas u orientaciones a transmitir a profesionales, industria y organizaciones sanitarias.

El compromiso de Akamai con la ciberseguridad del sector sanitario



Alberto Pérez
Experto en Seguridad de Akamai

Desde Akamai, nos enorgullece formar parte activa de la extraordinaria transformación digital que está experimentando el sector de la salud, contribuyendo con nuestro conocimiento y soluciones para mejorar la atención ciudadana, en lo que a ciberseguridad se refiere.

En la búsqueda de una atención médica más eficiente, tanto la Administración como las entidades farmacéuticas y otros proveedores de la industria están adoptando numerosas interacciones y transacciones digitales. No obstante, este proceso ha creado vulnerabilidades que los ciberdelincuentes están explotando con astucia con amenazas que podrían comprometer la seguridad del paciente.

> ***A diferencia de otros sectores líderes, la salud involucra a millones de trabajadores en tareas manuales y maneja millones de datos confidenciales de pacientes, convirtiéndose en un blanco preciado en Deep Web. En este contexto, la protección de datos se vuelve más crítica que nunca***

Las debilidades identificadas en el sector incluyen la persistencia de sistemas heredados no preparados para hacer frente a las sofisticadas tecnologías de ataque actuales, la recopilación masiva de datos digitales y la proliferación de APIs para cumplir con normativas gubernamentales y presiones de interoperabilidad. Además, en cuanto al sistema asistencial se refiere, la expansión de las modalidades de atención, como la atención a domicilio y las consultas virtuales, ha ampliado los límites tradicionales de la protección informática.

A diferencia de otros sectores líderes, la salud involucra a millones de trabajadores en tareas manuales y maneja millones de datos confidenciales de pacientes, convirtiéndose en un blanco preciado en Deep Web. En este contexto, la protección de datos se vuelve más crítica que nunca.

En Akamai, contamos con una solución innovadora para abordar estos desafíos: API Security. Esta herramienta proporciona visibilidad completa de todos los activos de API mediante una detección y supervisión continuas. Realiza auditorías de riesgos, identifica vulnerabilidades comunes y utiliza análisis de comportamiento para detectar amenazas y abusos de lógica en esta creciente superficie de ataque.



La solución, basada en SaaS independiente de plataformas, incorpora capacidades XDR a la seguridad de aplicaciones y API. Ofrece detección continua de API para crear una visión completa de la organización y sus activos, junto con auditoría de riesgos, clasificación de datos y puntuación de riesgo para todas las API. La detección avanzada de amenazas mediante IA y análisis del comportamiento, junto con información contextual sobre alertas, permite una respuesta personalizada a las amenazas, identificando riesgos que otros podrían pasar por alto.

En resumen, la transformación digital en el sector sanitario es un camino inevitable, pero debemos abordar sus desafíos con soluciones adaptadas y eficaces. Con API Security de Akamai, estamos comprometidos en proteger la "salud digital", asegurando que cada paso hacia adelante en este sector esté respaldado por una sólida barrera contra las amenazas cibernéticas.

Entornos seguros para los datos de salud



José Antonio Sánchez Ahumada
Sales Director Claroty/Medigate Iberia

Los datos son uno de los recursos más valiosos que tiene cualquier organización. Desde hace décadas o incluso siglos, quien tiene información y puede manejar datos que otros no tienen, se encuentra en una situación privilegiada respecto a los demás. Estos datos se pueden usar para innumerables cometidos y cada vez es más fácil acceder a la información desde cualquier dispositivo y lugar. Pero esta facilidad y accesibilidad tienen un precio: Los datos están más expuestos que nunca.

Hoy en día, una gran parte de los ciberataques se realizan para la obtención (de forma no lícita) de datos que luego se pueden utilizar para diferentes acciones. Por ello tenemos que ser conscientes de que una estrategia sólida de ciberseguridad debe tener la protección del dato como uno de sus pilares. Pero la protección del dato va más allá de protegerlo en su origen o en su almacenamiento. Hay que proteger todo el entorno donde puede estar presente.

> ***Debemos tratar los datos desde un punto de vista actual donde no podemos evitar que los datos viajen de un lado a otro, pero sí que podemos monitorizar y analizar por donde pueden estar viajando para mitigar los posibles ataques o sus consecuencias***

Los datos viajan por todos lados, y todavía más en los entornos hospitalarios donde se ha pasado de utilizar medios más tradicionales como la libreta y el bolígrafo a usar complejos sistemas de compartición de información que, aunque permitan que los profesionales compartan información de forma rápida y eficiente, también abren las puertas a los posibles atacantes. Según medios del sector, año tras año se incrementa el robo de datos de entornos relacionados con la salud. Desde 2009 hasta finales de 2023 se reportaron más de 5.880 filtraciones de datos de grandes organizaciones de la Salud. Las causas fueron varias: *ransomware*, incidentes de *hacking*, etc.

Por ello debemos tratar los datos desde un punto de vista actual donde no podemos evitar que los datos viajen de un lado a otro, pero sí que podemos monitorizar y analizar por donde pueden estar viajando para mitigar los posibles ataques o sus consecuencias. Así podremos anticiparnos a los ataques y mitigar o aminorar sus consecuencias ¿Cómo podemos hacerlo? A continuación, se describen los puntos clave para poder hacer frente a estas situaciones:

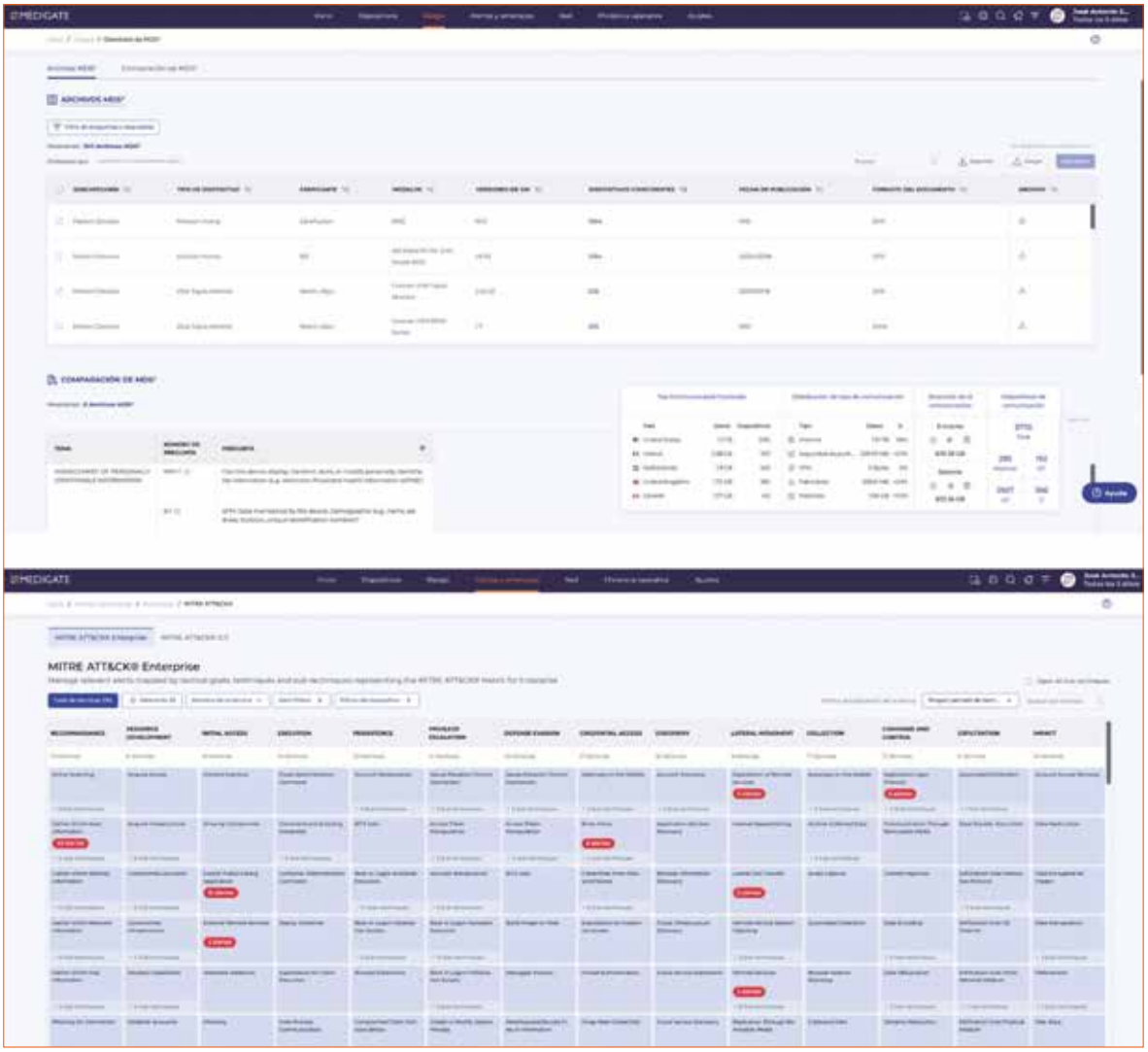
- Tener una visión global de todos los elementos o dispositivos a través de los cuales puede generarse o pasar la información que queremos proteger. En un Hospital contamos con equipamiento OT, IoT, IT, IoMT, etc y es necesario conocer cómo interactúan estos dispositivos entre sí. Cada día hay más interconexiones y los datos se generan y viajan por diferentes lugares.
- Contar con la posibilidad de poder ver diferen-

tes flujos de comunicación entre clientes, sistemas, etc para controlar que los flujos de datos son los permitidos. Si no conocemos este detalle no sabremos por dónde van los datos.

- Seguir las indicaciones de MDS2 (Manufacturer Disclosure Statement for Medical Device Security) para asegurarnos que el equipamiento médico que genera o consume datos, cumple con sus parámetros.
- Conocer si hay algún tipo de riesgo de fuga de información. Para ello se debe tener una visión de posibles equipos atacantes o posibles situaciones de riesgo.
- Segmentación. Empezar a desarrollar una estrategia de Segmentación para ayudar a reforzar los puntos anteriores.
- Integrar todo el ecosistema de soluciones de Ciberseguridad para cruzar información que permita evitar, contener o mitigar y reducir el alcance de situaciones provocadas para el robo de datos.

Hay otras muchas aproximaciones que complementan a esta. Pero si seguimos estos pasos, podremos estar seguros de que estamos creando una muy buena base para tener un entorno seguro para los datos de Salud. Pongamos todos de nuestra parte para que esto sea así.

Desde Claroty Medigate estaremos encantados de ayudar a nuestros clientes del entorno Sanitario en este momento tan importante para todo el sector. Cuenta con nosotros para recorrer juntos este camino.



Ciberseguridad integrada para la protección del dato sanitario



Alfredo Reino
Sr. Solution Architect, Global System Integrators CrowdStrike

En la era actual, donde la tecnología es la base y sustento de todos los procesos que afectan a nuestras vidas, la protección de datos personales y de salud se ha convertido en un pilar fundamental, especialmente en entornos sanitarios. La interconexión de sistemas, la recopilación masiva de datos y la transmisión electrónica de información médica han generado beneficios sin precedentes, pero también han planteado desafíos significativos en términos de seguridad y privacidad. En este contexto, la implementación de una ciberseguridad integrada se presenta como una necesidad imperante para salvaguardar la confidencialidad, integridad y disponibilidad de la información sensible.

PROTECCIÓN DE DATOS PERSONALES Y DE SALUD: UN DERECHO FUNDAMENTAL

La información de salud y los datos personales relacionados con el ámbito médico son sumamente sensibles y, por ende, requieren una protección rigurosa. Los registros médicos contienen detalles íntimos sobre la condición física, mental y emocional de los individuos, y su manejo inadecuado puede tener consecuencias devastadoras. La legislación y normativas, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea, subrayan la importancia de garantizar la privacidad y seguridad de estos datos, reconociendo el derecho fundamental a la protección de la información personal.

La complejidad creciente de las amenazas cibernéticas en el ámbito sanitario demanda un enfoque integral de ciberseguridad. Un sistema de protección integrada abarca la seguridad en diferentes niveles, desde el puesto de trabajo hasta la red perimetral y la información almacenada. Este enfoque holístico permite una detección más eficiente de posibles amenazas, un análisis profundo de incidentes y una respuesta automatizada para minimizar el impacto de los ataques.

CAPACIDADES DE DETECCIÓN Y ANÁLISIS EN DIFERENTES FRENTES

La primera línea de defensa reside en la capacidad de detectar posibles amenazas en múltiples frentes. En los puestos de trabajo y servidores, la implementación de medidas de seguridad, como soluciones EDR y de protección contra el malware, es esencial. A nivel de red perimetral, la monitorización constante y la identificación de comportamientos anómalos son cruciales. Además, la protección de datos en sí misma debe incluir mecanismos de detección temprana de accesos no autorizados o intentos de manipulación.

Plataformas como CrowdStrike Falcon que son capaces de integrar de forma holística la detección y protección contra amenazas son nuestras grandes aliadas, para simplificar el trabajo de nuestros equipos de seguridad y reducir la proliferación de soluciones de nicho, reduciendo así la complejidad de nuestra arquitectura de seguridad.

La ciberseguridad integrada no solo se trata de identificar amenazas, sino también de realizar un triaje para determinar su naturaleza y un análisis profundo para comprender su alcance e impacto. Herramientas de análisis avanzadas, usando la



inteligencia artificial y el aprendizaje automático, pueden desempeñar un papel fundamental en este proceso. Al comprender el comportamiento de las amenazas, las organizaciones sanitarias pueden mejorar sus medidas preventivas y fortalecer sus sistemas de seguridad.

RESPUESTA AUTOMATIZADA: LA CLAVE PARA MITIGAR RÁPIDAMENTE LOS INCIDENTES

La velocidad de respuesta es esencial en la ciberseguridad, y la automatización desempeña un papel crucial. El tiempo medio de detección se debería medir en minutos y no días.

Asimismo, el tiempo medio entre la intrusión inicial y el inicio de acciones significativas en el objetivo (exploración interna, escalado de privilegios, movimiento lateral, etc.) por parte de los adversarios, se ha reducido en los últimos años hasta valores cercanos a los 60 minutos, según el 2024 Global Threat Report de CrowdStrike, lo que nos marca un horizonte temporal que determina el "tempo" deseado de las acciones de contención y respuesta, y la necesidad de automatización para responder automáticamente a incidentes identificados, permitiendo a las instituciones de salud mitigar rápidamente las amenazas, reduciendo el tiempo de exposición y minimizando el impacto potencial en la integridad y confidencialidad de los datos.

En conclusión, la protección de datos personales y de salud en entornos sanitarios es esencial para preservar la confianza del paciente y garantizar la continuidad de la atención médica. La implementación de una ciberseguridad integrada, con capacidades de detección, análisis y respuesta automatizada, se presenta como una necesidad urgente en un mundo digital interconectado. Solo a través de este enfoque holístico se pueden enfrentar de manera efectiva los desafíos emergentes y garantizar la seguridad de la información médica.

¿Debe el sector sanitario (pre) ocuparse por la ciberseguridad?



Jordi Juan Guillem
Socio, Technology Consulting de EY

En una sociedad cada vez más digitalizada, los avances en la tecnología han permitido importantes progresos en la prestación de los servicios sanitarios. La medicina se ha ido adaptando a estos cambios beneficiándose de sus ventajas hasta el punto de que las operaciones robóticas a distancia o las consultas por videoconferencia, nos parecen conceptos totalmente cotidianos.

No es ajeno a nadie que, a día de hoy, los profesionales de la salud cuentan con el apoyo de asistentes de Inteligencia Artificial (IA) entrenados con prácticamente la totalidad de la literatura médica disponible, desde el Harrison de Medicina Interna, hasta el último tratado de medicina endocannabinoide. Y esto sólo acaba de empezar, dentro de muy poco veremos estos asistentes de IA enriquecidos con un amplio abanico de información individual del paciente y de su entorno: desde su historia clínica, su genoma o información de sus dispositivos "inteligentes" como *smartwatches,* hasta los análisis de fecales, el nivel de ruido o la calidad del aire de su barrio…

El inmenso potencial de estos avances tecnológicos promete catalizar una revolución en la prestación de servicios sanitarios, permitiendo una asistencia más personalizada y mejorando notablemente la eficiencia en los cuidados médicos. Sin embargo, este creciente flujo de información digital también está trayendo consigo nuevos retos y desafíos, principalmente en lo que afecta al acceso a la información y en el campo de la ciberseguridad.

En este contexto, nos vemos en la obligación de reflexionar sobre quién debe tener acceso a todos estos datos sensibles. ¿Debe ser sólo el personal sanitario, o también las farmacéuticas que desarrollan tratamientos específicos? ¿Y qué hay de las aseguradoras o incluso los empleadores? Y aunque cada uno de estos roles tiene su propia justificación, la pregunta más importante es: ¿dónde ponemos el límite? Los límites éticos, por supuesto, deben ser una consideración principal. Pero también, ¿quién decide y quién finalmente es dueño de toda esta información? El "Data Act", que entró en vigor en la Unión Europea el pasado mes de enero, establece directrices para el uso primario y secundario de los datos sanitarios, pero habrá que esperar a su implantación efectiva para poder valorar sus efectos e implicaciones.

Por otro lado, esta creciente acumulación de datos de alto valor para la prestación de servicios sanitarios también atrae el acecho constante del cibercrimen. Los registros médicos contienen información personal detallada y altamente confidencial, mientras que la información sobre enfermedades, tratamientos y patrones de salud pueden tener un gran valor comercial en el mercado negro, por lo que a menudo son objeto de ataques de ciberseguridad. De ahí la importancia crucial de contar con sólidos mecanismos de protección de la información, control de accesos y técnicas de anonimización.

Los ciberataques en el sector sanitario están en el orden del día, siendo el penúltimo, el ataque por *ransomware* (tipo de ataque que bloquea los datos de una víctima y amenaza con mantenerlos bloqueados, a menos que la víctima pague un rescate) sufrido por Change Healthcare (empresa que centraliza gran parte de la gestión de pagos y recetas médicas en Estados Unidos) el pasado 21 de febrero. Según la Asociación de Hospitales de EE.UU. (AMA por sus siglas en inglés), este inci-

dente es "el mayor ciberataque perpetrado contra el sistema sanitario estadounidense en toda su historia". Este ataque provocó la interrupción de servicios cruciales durante semanas, lo que llevó a que cientos de hospitales y centros médicos en todo el país no pudieran emitir recetas ni procesar pagos, entre otras muchas funciones vitales. Esta situación generó un gran malestar en la población y se reflejó rápidamente en las redes sociales, donde los pacientes compartieron su frustración por no poder acceder a sus medicamentos. Hay indicios de que Change Healthcare pudo haber pagado un rescate de 22 millones de dólares al grupo de *ransomware* BlackCat para recuperar el control de sus datos. De confirmarse este pago, no haría más que amplificar el mensaje de la rentabilidad de los ataques contra el sector sanitario, y si hay algo que caracteriza a los grupos de cibercriminales, es que son altamente predecibles, si descubren un sector rentable, como este, repetirán sus ataques una y otra vez, de forma sistemática.

Por suerte o por desgracia, la naturaleza compleja y multifacética del sistema sanitario español -con competencias descentralizadas y una combinación de proveedores de servicios sanitarios públicos y privados- podría, en principio, ser vista como una barrera contra la materialización ciberataques con un impacto estructural tan elevado como el sufrido por Change Healthcare. Sin embargo, esta aparente fortaleza no está exenta de sus propias vulnerabilidades derivadas de la asimetría en la que se protegen los distintos actores que conforman el Sistema Nacional de Salud.

Por un lado, el que la prestación asistencial pública se realice desde las Comunidades Autónomas, propicia la coexistencia de niveles de madurez en ciberseguridad heterogéneos. Mientras que algunos servicios de salud cuentan con robustas estructuras de ciberseguridad especializadas y dedicadas, otros consumen los servicios de ciberseguridad transversales que les presta su Comunidad Autónoma.

Por otro lado, los proveedores de servicios sanitarios del sector privado poseen sus propias medidas de seguridad, que pueden ser tan variadas como numerosos son los actores privados en el sector.

Esta heterogeneidad podría producir brechas fácilmente explotables por ciberdelincuentes, quienes podrían enfocar sus esfuerzos en aquellos puntos del sistema que consideren más vulnerables para maximizar el retorno de su inversión.

La omnipresente amenaza del cibercrimen enfatiza la importancia de contar una estrategia de ciberseguridad sólida y específica para el Sistema Nacional de Salud (necesidad que ya aflora la OCDE en su informe "*Health at a Glance 2023*", publicado el pasado mes de noviembre). Un aspecto crucial de esta estrategia debería ser el lograr tener visibilidad de los distintos niveles de madurez en ciberseguridad de todos los actores que componen el sistema, desde los proveedores de atención sanitaria públicos y privados hasta las diversas estructuras dentro de las Comunidades Autónomas.

Esta comprensión del ecosistema sanitario permitiría identificar tanto las fortalezas como las áreas de mejora o de vulnerabilidad dentro del sistema que los ciberdelincuentes podrían explotar. Adicionalmente, proporcionaría una imagen clara de dónde se necesitan mejoras y refuerzos en términos de protección de datos y seguridad de la información.

En este sentido, es fundamental establecer una hoja de ruta estratégica para unificar el nivel de protección a través de todo el sistema sanitario. Esta estrategia debe buscar no solo abordar las áreas de debilidad detectadas, sino también anticiparse a las futuras amenazas y evoluciones en el ámbito del cibercrimen. Además, la hoja de ruta debe definir e incorporar estándares de seguridad de la información que se espera que todos los actores del sistema cumplan.

Los ciberataques a los sistemas de salud no sólo acarrean graves consecuencias financieras, sino que también ponen en riesgo la atención al paciente y la prestación de servicios sanitarios esenciales. Por ello, contar con una estrategia de ciberseguridad sólida y adaptativa es esencial para proteger los datos de los pacientes, las infraestructuras críticas y, en última instancia, la salud pública en su conjunto. En un mundo cada vez más digitalizado y con amenazas cada vez más sofisticadas, la ciberseguridad debe ser reconocida como una prioridad dentro del sector sanitario.

La receta ante una epidemia de *ransomware*: seguridad integrada



Gorka Sainz
Director Systems Engineering Fortinet Iberia

Los últimos años han sido extremadamente duros para los proveedores de atención sanitaria. Por si la pandemia mundial no hubiera sido suficiente desafío, el sector sufre su propia epidemia de ataques de *ransomware*.

Las organizaciones sanitarias siempre han sido un objetivo atractivo para los ciberdelincuentes y sus ataques han tenido graves consecuencias. Los ataques de *ransomware* pueden provocar la caída de sistemas enteros y cortar el acceso informático a servicios esenciales. Lo más preocupante es el impacto que un ataque exitoso puede tener en los pacientes y su capacidad para acceder a la atención médica. Conocer el *modus operandi* de estos ataques es el primer paso para luchar contra ellos.

El *ransomware* tradicional persigue los datos, bloqueando los archivos hasta que se paga el rescate. Con la aparición de los dispositivos del Internet de las Cosas (IoT), ha surgido una nueva variedad de *ransomware*. No persigue los datos de una organización, sino que se dirige a los sistemas de control (por ejemplo, vehículos, líneas de montaje de fabricación, sistemas de energía) y los apaga hasta que se paga el rescate. En el sector sanitario, los ciberdelincuentes están atacando el Internet de las Cosas Médicas (IoMT) de la misma manera. Las organizaciones sanitarias cuentan con cientos de tecnologías operativas y dispositivos IoMT en juego, desde monitores de pacientes hasta dispositivos de diagnóstico por imagen, bombas de infusión e incluso sistemas de calefacción, ventilación y aire acondicionado.

Cualquiera de estos dispositivos conectados puede ser pirateado para acceder a los sistemas de información críticos de una organización sanitaria.

¿QUÉ HAY DETRÁS DEL VERTIGINOSO AUMENTO DEL RANSOMWARE EN EL ÁMBITO SANITARIO?

Las tres razones principales de su crecimiento son: el Ransomware-as-a-Service (RaaS), la obtención de rescates cada vez mayores procedentes de grandes objetivos (también conocido como "Big Game Hunting") y las amenazas sobre la revelación de los datos comprometidos si no se cumplen las demandas.

El *ransomware* como servicio y la venta de nombres de empresas que ya han sido comprometidas han mercantilizado el proceso delictivo. Un atacante novato, que actúa como si de un franquiciado de una organización delictiva se tratara, puede perpetrar con éxito su ataque a organizaciones sanitarias con escasos o nulos conocimientos técnicos.

Todos los procesos secundarios, desde la captación de objetivos hasta la fijación de precios y la recaudación de fondos, son ofrecidos bajo un modelo de servicio de pago por sofisticadas empresas delictivas que incluso prestan servicios de asistencia a sus cómplices.

Los enormes beneficios que el *ransomware* proporciona a los atacantes es *vox populi*. Esto ha desencadenado una "fiebre del oro malicioso" hacia organizaciones e industrias vulnerables, tanto por parte de ciberdelincuentes veteranos como de aspirantes. Los actores de amenazas estudian sus objetivos antes de lanzar un ataque y una vez que entran en la red de la víctima son pacientes, pueden pasar meses buscando los datos de alto valor que les permitirá obtener un rescate desorbitado.

Esta "caza mayor" persigue a organizaciones especialmente sensibles a las que un tiempo de inactividad prolongado arruina sus negocios y/o su reputación. Los ciberdelincuentes saben que es mucho más probable que estas empresas paguen rescates de mayor cuantía. Este es el caso del sector sanitario.

Por otro lado, uno de los aspectos más preocupantes de los últimos ataques de *ransomware* es la exfiltración de datos y la amenaza de liberarlos si no se paga un rescate. Algunas víctimas informaron de incidentes en los que los atacantes alegaban falsamente el robo de datos y luego intentaban asustarles para que pagaran un rescate. En otros casos, cuando las víctimas pagaron para que los atacantes eliminaran los datos robados, éstos renegaron y, en su lugar, filtraron o vendieron los datos de todos modos. En casos aún más graves, hemos visto cómo el *ransomware* destruía la red de una víctima borrando los discos de ordenadores de sobremesa y servidores, ¡a pesar de haber pagado el rescate!.

Para las organizaciones sanitarias, este es un ejemplo perfecto de por qué incluso las copias de seguridad de datos sólidas por sí solas no son protección suficiente contra las demandas de *ransomware*.

Parece evidente que los proveedores sanitarios y sus CISO necesitan diseñar, construir e instalar mejores defensas contra el *ransomware*, especialmente a medida que los ataques se hacen más frecuentes y dañinos. Los responsables de seguridad informática deben desplegar protecciones con capacidad para adelantarse a la actividad criminal y proteger a las organizaciones antes, durante y después de un ataque. Y que todas ellas "hablen entre sí".



UN ENFOQUE INTEGRADO ES EL CUIDADO CRÍTICO REQUERIDO

Muchas entidades maduras ya cuentan con planes de respuesta a incidentes, pero para reducir el riesgo y el alcance de las potenciales amenazas es necesario aplicar también otras estrategias proactivas. Cuando una organización se encuentra en medio de un ataque de *ransomware*, ya es demasiado tarde para poner en marcha los planes, procesos y tecnologías proactivas necesarias para detener el daño.

Obviamente, la planificación y la preparación antes de que se produzca un ataque es siempre una medida inteligente. Otro acierto es contar con una estrategia global de seguridad que incluya procesos y controles de seguridad integrados en cada etapa de la cadena del ataque.

Para protegerse eficazmente contra el *ransomware*, se requiere un enfoque integrado. Aunque hay una amplia gama de tecnologías de seguridad disponibles para reducir el riesgo y el impacto del ataque, si no funcionan juntas, se producirán lagunas por las que los delincuentes podrán desplegar su *malware*.

Independientemente de su calidad y funcionalidades, los productos por sí solos nunca proporcionarán el mismo nivel de prevención, detección y respuesta que un sistema totalmente integrado. En definitiva, las organizaciones sanitarias además de evaluar la eficacia de los controles de seguridad de red, correo electrónico, *sandbox*, web y *endpoint* individualmente, deben valora cómo operan conjuntamente estas para proporcionar una protección más sólida, rápida y gestionable a sus redes frente al *ransomware*.

El reto de la protección del dato de salud



Jesús María Doña Fernández
Director de Desarrollo de Negocio en Ciberseguridad socio-sanitaria Fujitsu

La invencibilidad es una cuestión de defensa... Así pues, los buenos guerreros toman posición en un terreno en el que no pueden perder, y no pasan por alto las condiciones que hacen a su adversario proclive a la derrota... Esta es la diferencia entre los que tienen estrategia y los que no tienen planes premeditados. **El Arte de la Guerra, Sun Tzu, siglo V a.C.**

El uso de los datos de salud representa un desafío desde el punto de vista de la ciberseguridad del paciente, no sólo por el carácter de especial sensibilidad de esta información sino por la propia repercusión que puede tener en la calidad de vida del ciudadano tanto por su uso en tratamientos (que esté recibiendo o futuros), como por su utilización fraudulenta en otros ámbitos fuera del sanitario y que puede poner en riesgo, como indica la OMS, la propia vida del paciente.

Para poder dimensionar el impacto, la importancia y los riesgos del dato de salud en la sociedad debemos tener claro a qué ámbitos nos estamos refiriendo, de forma muy general los podemos agrupar en tres grandes bloques:

i. **Datos relativos a la atención médica.** Es decir, la información demográfica del paciente y su identificación unívoca, así como, en muchos casos, información no clínica, como por ejemplo datos financieros o bancarios para el cobro de la asistencia.

ii. **Datos de la gestión de la salud.** Donde incluiríamos, a nivel individual, toda la información relacionada con el diagnóstico y tratamiento del paciente. Y a nivel global los datos que se usan para monitorear la salud y bienestar de la población, así como para diseñar intervenciones para la identificación de grupos de riesgo y mejora de la calidad de vida de las personas.

iii. **Datos investigación biomédica o de uso secundario.** Usados en la investigación, ensayos clínicos y formación para desarrollar nuevas terapias, medicamentos y procedimientos médicos o para evaluar la seguridad y eficacia de existentes, y que incluyen usos diferentes de lo que es propia atención médica del paciente.

Además, podemos añadir un nuevo tipo de datos que empieza a estar presente en todos los anteriores: la *información genómica.* Que precisamente por su especificidad y relevancia va a estar involucrada a corto plazo en todo el proceso de salud relacionado con el paciente, la gestión de la salud poblacional y la investigación posibilitando el paso a una verdadera sanidad personalizada.

Como vemos, hablamos de una información muy relevante, tanto desde el punto de vista individual del paciente como de sociedad y por lo tanto es una información muy valiosa por su potencial de cara al crimen organizado, que ve la oportunidad de obtener ingentes beneficios del sector de la salud a través de actividades vinculadas a los aspectos básicos de la información como son la confidencialidad, la integridad, la disponibilidad y la autenticidad, que se materializan en situaciones de extorsión, venta de información para su uso delictivo en otros ámbitos y contextos, robo de credenciales y suplantación de identidad, modificación de resultados clínicos y de tratamientos, rapto de sistemas de salud, bloqueo de quirófanos, paradas en la atención sanitaria básica, influencia en sector farmacéutico, etcétera.

La superficie de ataque usada por esta ciberdelincuencia que pone en jaque los sistemas de salud aprovecha las debilidades de un sistema que crece de forma continuada y no siempre coordinada desde el punto de vista de las tecnologías de la información y la ciberseguridad, lo que ha generado una superficie de exposición muy amplia en la que se incluyen los sistemas hardware TI tradicionales, los nuevos perímetros que se amplían o desaparecen con la incorporación de la nube y nuevas formas de trabajo y comunicación-monitorización de los pacientes y profesionales, los servicios publicados en internet, las aplicaciones sanitarias, los dispositivos relacionados con tecnologías de la operación y que están muy presentes en la gestión de los centros sociosanitarios, la electromedicina, la inteligencia artificial, y un largo etcétera que es muy estudiado y conocido por la ciberdelincuencia y que muchas veces, desde los propios centros de gestión y responsabilidad de las instituciones, se desconoce o no se quiere conocer por el miedo a ver las deficiencias y debilidades que se esconden "*debajo de la alfombra.*".

Precisamente, el objetivo de las empresas que proveen servicios de ciberseguridad debe ser ayudar a vencer ese miedo para dar visibilidad a todos los puntos débiles y fuertes para poder enfocarse en desarrollar estrategias efectivas y crear defensas que permitan preservar estos pilares básicos que antes enumerábamos y gestionar y monitorizar todos los sistemas vinculados a la atención sociosanitaria y al dato de salud, aplicando tecnologías avanzadas como la inteligencia artificial o el aprendizaje automático (*machine learning*), y la adecuación y aplicación de normativas tanto nacionales como internacionales que permiten mejorar y auditar nuestros servicios-sistemas de salud.

Para ello, es clave poner el foco, de forma general y resumida, en las siguientes líneas básicas:

- La aplicación estricta de metodologías contrastadas y buenas prácticas en el desarrollo del software sanitario, nuevas tecnologías disruptivas (como la inteligencia artificial) y aplicaciones vinculadas a la salud, que deben alejarse del concepto de desarrollo artesanal dando paso, de una vez por todas, a la industrialización de los procesos de desarrollo, implementado controles de calidad y pruebas no sólo desde el punto de vista funcional, sino también desde el de la ciberseguridad, aplicando conceptos como la seguridad por defecto, mínimo privilegio y la confianza cero de una vez por todas. A todo esto, ayudará la necesidad de acreditación y cumplimiento estricto de la normativa europea sobre productos sanitarios que se debe aplicar a todo sistema software y *hardware* que se use en el ámbito de la asistencia sanitaria.
- La adecuada instalación, gestión, configuración y bastionado de las tecnologías vinculadas a la salud, en la que surgen siglas como la TI, TO, IoT y la IoMT que, como ya se ha indicado, no hacen más que ampliar las superficies de exposición y riesgo y dificultan el control tradicional de la seguridad al superar los dispositivos médicos la barrera física de los centros sociosanitarios, pasando a la nube e incluso a los hogares y dispositivos personales de los pacientes. Todo esto nos obliga a desarrollar, conocer, implementar y aplicar nuevas metodologías de protección global que nos permitan si no estar un paso por delante de la ciberdelincuencia, al menos al mismo nivel.
- Y finalmente, las personas, donde ya se debe incluir a todos los profesionales sociosanitarios (personal de mantenimiento de los edificios, celadores, alumnos en prácticas, personal sanitario, gerencias, ...) y al propio paciente y su entorno, lo que hace necesaria una formación y concienciación social tanto específica como global que permita un uso correcto de la tecnología en aras de la protección del paciente, la salud y la información sanitaria con el objetivo final de posibilitar una sociedad más segura y una sanidad confiable, eficiente y eficaz.

Todo esto implica un reto y desafío tanto para las administraciones como para todas las entidades y profesionales sociosanitarios que deben ver en las empresas de servicios de ciberseguridad un aliado que aporte el conocimiento, la experiencia y las herramientas más modernas y adecuadas para la protección del dato sanitario y por ende de los profesionales, los pacientes y la sociedad en general.

Capture información sobre el tráfico para monitorear y proteger los entornos de IT sanitarios. Lecciones extraídas de experiencias reales



Alex López de Atxer
Regional Sale Manager Gigamon

Durante los últimos tres años he tenido la oportunidad de participar en varios proyectos de captura de tráfico para su análisis con sondas de monitorización y seguridad en entornos IT sanitarios, así como en el posterior despliegue de algunos de estos proyectos. Esto me ha permitido encontrar algunas de las claves del éxito de estas iniciativas, tanto del punto de vista técnico como económico.

EXPERIENCIA 1: GRUPO HOSPITALARIO PRIVADO

El primer proyecto en el que participé tenía como objetivo desplegar múltiples sondas de seguridad para un grupo hospitalario privado compuesto por casi cincuenta hospitales y un centenar de clínicas y centros más pequeños. Entre estas sondas se encontraban un NAC (Network Access Controller), una sonda de seguridad OT/IoT y un Network Detection and Response (NDR).

Después de analizar varios centros, pudimos ver que la topología de las redes de los centros era de lo más variado y no seguían en origen una política IT común, fruto de provenir de distintas adquisiciones a lo largo de los años, o a despliegues de redes orquestados por el propio centro sin un diseño homogéneo del grupo.

La más significativo fue sin duda la ausencia de *firewalls* en muchos de estos centros, lo que les obligaba a desplegar múltiples puntos de captura de tráfico para dirigirlo a las sondas objeto del proyecto, generando un coste prohibitivo.

Más allá de la obviedad de que el primer paso para poder securizar un entorno IT es la segmentación de red, el disponer de un equipo que haga de *default Gateway* de la red nos va a permitir tener acceso de todo el tráfico entre departamentos. Esto se logra simplemente capturando los interfaces de entrada y salida de este equipo mediante TAPs de una manera sencilla y económica.

En el caso de que existan alguna VLans interesantes para el proyecto, y que por tanto sea necesario ver el tráfico entre equipos de esta VLAN (InterVLAN), se puede hacer algún *port mirror / SPAN* específico y agregarlo con el resto de tráfico proveniente de los TAPs. Sin embargo, es importante tener en cuenta que los *SPAN/mirrors* no son nunca una opción preferible por su ineficacia y carga de procesamiento extra sobre los equipos en los que se activa.

EXPERIENCIA 2: IBSALUT

Dentro de la iniciativa de CiberAP he tenido la oportunidad de participar en el piloto y posterior despliegue de la solución de captura de tráfico utilizando Network Packet Brokers (NPB) para su análisis sobre numerosas sondas de visibilidad y seguridad (OT/IoT, CCN, NDR, NPM).

En este caso, la captura de tráfico se llevó a cabo en los siete hospitales regionales de referencia y los dos CPDs, con la particularidad de ser las conexiones por cable submarino entre las islas

Por tanto, la principal limitación que hemos encontrado ha sido los anchos de banda de conexión entre los diferentes hospitales. Para afrontar este reto, tuvimos que colaborar con el operador de comunicaciones para poder mancar el tráfico de visibilidad y así poder **establecer Calidad de Servicio QoS en la red MPLS** de interconexión. Esto implicó priorizar el tráfico de producción por encima de las copias de tráfico destinadas a las sondas. Otro hallazgo importante al que llegamos fue saber que había una MPLS de *backup*, que en condiciones normales no cursaba tráfico de producción, por lo que se tomó la decisión de usar esta red siempre que fuera posible para el tráfico a enviar a las herramientas de monitorización.

Este proyecto también sirvió para hacer un exhaustivo análisis de las **técnicas de reducción de tráfico y su impacto en las herramientas de visibilidad.** Estas técnicas se basan en filtros de nivel 2-3-4 y manipulados avanzados de los paquetes de cara a optimizar el rendimiento de las sondas, salvaguardando las comunicaciones. Por ejemplo, técnicas como el *slicing* (eliminación de cabeceras) se ha mostrado muy eficaz para sondas de visibilidad, que no requieren del *payload*. *Advanced Slicing* (envió de los XX primeros paquetes de una sesión, descarte del resto) son ideales para tratar el protocolo DICOM (y similares), ya que en las cabeceras del protocolo esta la información relevante para las sondas de OT/IoT.

Finalmente, la posibilidad de desplegar **sondas locales en cada centro o su centralización en el CPD** nos ha mostrado las ventajas y desventajas de cada opción: alta visibilidad a coste alto de *capex* y *opex* en el primer caso, interesantes para seguridad, y menos visibilidad a muy bajo coste de *capex* y *opex* en el segundo, ideal para monitorización.

EXPERIENCIA 3: COMUNIDAD AUTÓNOMA 1

En esta tercera experiencia, exploramos una comunidad que cuenta con una treintena de hospitales, donde si existía una homogenización de

> ***Este proyecto sirvió para hacer un exhaustivo análisis de las técnicas de reducción de tráfico y su impacto en las herramientas de visibilidad***

redes. Vemos características interesantes, como que las salas de comunicaciones se encuentran divididas en dos cuartos en muchas ocasiones, con escasas fibras de interconexión entre ellas. Para resolver este escenario, se implementan equipos **agregadores de bajo coste en la sala remota.** Estos equipos envían el tráfico agregado y prefiltrado por un par de fibras a la sala principal, donde se agregará a su vez con todo el tráfico captura en la sala principal.

EXPERIENCIA 4: COMUNIDAD AUTÓNOMA 2

En este caso, nos hemos enfrentado a tener que capturar tráfico en una extensa red hospitalaria de más de ochenta centros principales, y varios cientos de secundarios e incluso algún millar de centros en total.

La complejidad de esta red y el potencial coste significativo de CAPEX y OPEX que puede suponer una mala estrategia de captura de tráfico nos hace reflexionar sobre la regionalización de las sondas en cabeceras provinciales. Además, se plantea el uso de **técnicas más agresivas de reducción de tráfico,** como el filtrado L7, generación de metadatos y el *Slicing Avanzado*, que a su vez salvaguarden la red.

Tras un **análisis pormenorizado de los flujos de red,** buscando minimizar los puntos de captura de tráfico, hemos podido observar que la propia red lógica tiene una topología de árbol, y que unos centros dependen de otros a nivel IT y, por tanto, capturando en el centro de referencia, ya estamos capturando de facto el tráfico en las sedes que dependen de estos.

Por último, para centros de menor tamaño, y donde se quiera tener cierto nivel de visibilidad, la solución de **NPB virtualizados sobre barebones** de bajo coste se ha mostrado como la más eficiente.

Tecnología digital para la medicina personalizada: biogenética y redes federadas de datos



Inmaculada Pérez Garro
Directora de Salud Digital de Secure e-Solutions de GMV

Las agencias del medicamento española y europea ya aconsejan el uso de biomarcadores genéticos para prevenir fallos terapéuticos, interacciones y reacciones adversas, ofreciendo recomendaciones para su prescripción, acorde con la aplicación de una medicina personalizada. Porque la respuesta de una persona a uno u otro fármaco no es homogénea. El análisis de los genes, junto a otras variables, ofrece indicaciones para la prescripción más acertada y contribuye a mejorar la eficacia y seguridad de los medicamentos. La farmacogenética puede mejorar los resultados de salud y personalizar los tratamientos.

La tecnología digital de última generación ha conseguido proporcionar a los especialistas sistemas de apoyo a la decisión con un nivel científico tan elevado, que incluso se pudiera evitar consultar, por ejemplo, las fichas de los miles de productos de la Agencia Española del Medicamento para decidir una prescripción. Lo que explica la apuesta del Servicio Extremeño de salud con el proyecto MedeA, que promueve la incorporación al Servicio Nacional de Salud (SNS) de herramientas digitales innovadoras para la toma de decisiones clínicas en la prescripción personalizada de medicamentos.

Los programas existentes hoy en día están basados, en su mayoría, en el análisis de un solo gen y un único fármaco. Sin embargo, MedeA, contempla varios genes y varios fármacos, además de las condiciones clínicas e interacciones farmacológicas. Así, como explica el Dr. Llerena, «en vez de prescribir sólo en base a criterios clínicos, antes de seleccionar uno de estos fármacos, el especialista tendrá la posibilidad de utilizar la información del análisis genético del paciente, y consultar después de forma automática a través del Sistema de prescripción personalizada PoPS, la información necesaria para personalizar el tratamiento. Este es el gran logro de PoPS: combinar información proveniente de varios fármacos, varios genes y varios factores clínicos para elegir la mejor combinación".

El *Personalized Oriented Drug Prescription System o* sistema de prescripción personalizada que ha sido desarrollado con tecnología de GMV incluye variantes clínicas junto a las genéticas en politerapia, optimizando la medicación que toma el paciente. «PoPS facilitará en primera instancia seleccionar qué medicamentos van a ser más efectivos para el paciente, la mejor combinación de entre las posibles, qué dosis es la más recomendable y qué fármacos no debería tomar para evitar reacciones adversas, prevenir interacciones y fallos terapéuticos», explica el Dr. Llerena. MedeA, es un proyecto ambicioso que se ha desarrollado en Extremadura, como un subgrupo representativo de la población europea, y como prueba piloto por las características de esta comunidad autónoma (sistema de salud único, homogéneo y con población reducida).



REDES FEDERADAS PARA INVESTIGACIÓN FARMACOLÓGICA

En la investigación farmacológica, también la tecnología digital como la IA ha supuesto un gran avance para explotar grandes volúmenes de datos. Para ello, GMV propone un enfoque basado en la creación de redes federadas seguras que conecten entre sí espacios de datos masivos. La principal ventaja que proporcionan las redes es la mejora de la calidad de los modelos matemáticos que se usan en *machine learning* porque ésta depende del volumen de datos accesibles y de su heterogeneidad, aspectos que se ven reforzados al agregar tantas fuentes de información. Así, disponer de una red federada permite entrenar modelos nuevos con patologías que hasta ahora no había sido posible (como enfermedades raras) y hacerlos más precisos y específicos, acordes al contexto sociodemográfico de cada paciente, ciudadano o localidad. Además, al disponer de datos de personas de diferentes poblaciones, estilos de vida y servicios de salud seremos capaces de reducir el sesgo discriminatorio que padecen muchos de los algoritmos actuales.

Otro de los beneficios que conlleva el uso de redes federadas es que permiten compartir el gasto económico, humano y medioambiental que acarrean la producción y la gobernanza de la información, siendo factible el reparto de los costes derivados del esfuerzo tecnológico, la computación, los procesos y la seguridad. Asimismo, de gran importancia en el ámbito de la salud, es la capacidad retrospectiva-prospectiva que nos pueden proporcionar las redes de datos. Un ejemplo concreto lo encontramos en el caso de estudios observacionales, donde ponemos analizar variables antes y después de una determinada enfermedad.

Cartera EUDI: Revolucionando la identidad europea



Alberto Martín de los Santos
Director de Ciberseguridad en Inetum

INTRODUCCIÓN

La Cartera Europea de Identidad Digital (EUDI Wallet) es una iniciativa innovadora que transformará la forma en que los ciudadanos europeos se identifican y gestionan sus datos personales en el ámbito digital. Esta iniciativa, impulsada por la Comisión Europea dentro de eIDAS2, tiene como objetivo crear una solución única y segura que permita a los ciudadanos acceder a una amplia gama de servicios públicos y privados en toda la Unión Europea.

La Cartera EUDI se compone de tres elementos principales:

- Identidad digital: Permite a los ciudadanos identificarse de forma segura en línea y fuera de línea, utilizando su documento de identidad nacional o un certificado de identificación electrónica.
- Atributos personales: Almacena información personal como la edad, la dirección o el estado civil, que puede ser compartida con los servicios que lo requieran, con el consentimiento del usuario.
- Firma electrónica: Permite a los ciudadanos firmar documentos digitales de forma segura y legalmente vinculante.

El proyecto se encuentra en una fase crucial en estos momentos. A partir de febrero de 2024, 14 estados miembros han comenzado la fase de pruebas, mientras que otros 12 están en proceso de implementación. Se espera que la Cartera EUDI esté disponible para todos los ciudadanos europeos en los próximos meses según la agenda prevista, y la Comisión Europea estima que para 2030 el 80% de los ciudadanos de la UE dispongan de la misma.

La Cartera ofrece una mejora en seguridad, comodidad, privacidad y eficiencia para los ciudadanos, las empresas y las administraciones públicas de la UE.

CUATRO PILOTOS DE GRAN ALCANCE

Para probar la viabilidad y el impacto de la Cartera EUDI en diferentes contextos, se han implementado cuatro proyectos piloto a gran escala europea:

1. **CEE:** Este proyecto se centra en la interoperabilidad transfronteriza, permitiendo a los ciudadanos utilizar su identidad digital para acceder a servicios públicos en otros países de la UE.
2. **NOBID:** Se centra en el uso de la Cartera EUDI para acceder a servicios de banca online y pagos electrónicos.
3. **DC4EU:** Se enfoca en el uso de la autenticación en el ámbito de la educación y la investigación.
4. **Potential:** Este proyecto desarrolla el uso de la Cartera EUDI para la gestión de datos personales y el consentimiento en el sector sanitario.

EPRESCRIPTION: UN CASO DE USO INNOVADOR

La ePrescription, o receta electrónica, es uno de los casos de uso más relevantes dentro del piloto



Potential y la Cartera EUDI. Permite a los médicos y farmacéuticos emitir y gestionar recetas electrónicas de forma segura y digital, simplificando el proceso para pacientes y profesionales de la salud. La Cartera empodera al paciente en el ámbito de la salud de las siguientes maneras:

- Acceso instantáneo a la información: los pacientes pueden acceder a sus recetas electrónicas, historial médico y otros datos relevantes en cualquier momento y lugar.
- Mejora de la seguridad: la cartera protege la información médica de los pacientes contra el robo y la falsificación.
- Mayor control: los pacientes tienen control total sobre sus datos y pueden elegir con quién compartirlos.
- Interoperabilidad transfronteriza: permite a los pacientes utilizar sus recetas electrónicas en cualquier país de la UE.

La ePrescription tiene el potencial de generar un impacto social y económico, facilitando la calidad de vida de los pacientes y evitando errores en la prescripción y dispensación de medicamentos y materiales sanitarios, e igualmente, reduciendo los costes asociados a la engorrosa gestión manual.

Sin embargo, su implementación también enfrenta algunos retos como son el lograr la interoperabilidad técnica y legal entre diferentes países y sistemas de salud, el asegurar la protección de los datos personales de los pacientes o la aceptación por parte de los profesionales de la salud y especialmente de los pacientes. Los resultados de proyectos piloto como ePrescription, son fundamentales para un despliegue satisfactorio de la Cartera EUDI en toda la UE.

ASPECTOS CLAVES PARA CONSIDERAR

Finalmente, se deben tener en cuenta algunos puntos para que la implantación de la Cartera EUDI tenga éxito:

- Un aspecto fundamental de la Cartera EUDI es la seguridad y privacidad de los datos personales. Se deben implantar medidas robustas para proteger la información de los usuarios contra el robo, la falsificación y el fraude.
- La Cartera EUDI debe ser interoperable entre los diferentes países y proveedores de servicios para garantizar su uso en toda la UE.
- Debe ser accesible para todos los ciudadanos, independientemente de su edad, habilidades digitales o condición socioeconómica.
- Es fundamental generar confianza entre los ciudadanos y las empresas para que sea ampliamente adoptada.

Malware y robo de datos: 2023, un año convulso para la ciberseguridad en el sector salud



Miguel Ángel Martos
Country Manager Iberia Netskope

Hace apenas unas semanas, Netskope Threat Labs ha publicado su último informe sobre el sector salud en el que se analiza la adopción de aplicaciones en la nube y las principales tendencias de *malware* en el sector. El informe ha sido elaborado a partir de datos de uso anonimizados recopilados sobre un subconjunto del sector sanitario de entre los más de 2.500 clientes de Netskope, todos los cuales han dado su autorización previa para que sus datos sean analizados de esta manera.

Con análisis en profundidad sobre las amenazas relacionadas con la nube -incluyendo *phishing* en la nube, estafas, entrega de *malware*, comando y control, exfiltración de datos, exposición de datos- estos laboratorios ayudan a proteger a los clientes de Netskope de actores maliciosos y contribuyen a la comunidad global de seguridad con investigación, asesoramiento y mejores prácticas.

Durante 2023, el informe de Netskope Threat Labs destaca que la industria de la salud ha sido uno de los objetivos preferidos de los cibercriminales, sufriendo alguna de las principales mega brechas que se pudieron ver el año pasado, brechas en las que se llegó a superar el millón de registros robados. En concreto, dos de las mayores brechas del año consiguieron con éxito hacerse con 11 millones y 9 millones de datos en dos ataques, uno dirigido contra los hospitales HCA Healthcare y la segunda contra la aseguradora MCNA (Managed Care of North America).

El informe también examina el incremento sostenido en la adopción de aplicaciones en la nube así como las tendencias del *malware* en el sector. En concreto, el número promedio de aplicaciones en la nube con las que actúan los usuarios ya son 22.

Entre las principales conclusiones del informe se destaca el papel dominante que Infostealers ha tenido como la principal familia de *malware* y *ransomware* dirigido contra el sector sanitario, con la que los atacantes intentan robar datos valiosos de entidades y pacientes para luego chantajear o pedir un rescate. Entre los atacantes, el grupo de *ransomware* Clopp fue especialmente activo atacando entidades sanitarias y aseguradoras médicas, aprovechando la vulnerabilidad CVE-2023-34362 MOVEit .

Las descargas de *malware* aumentaron en 2023, estabilizándose en el segundo semestre. El *malware* distribuido a través de la nube acabó el año representando el 40% aproximadamente del total de descargas de *malware* en el sector sanitario, tras el máximo del 50 % en junio, y luego descendiendo ligeramente en la segunda mitad del año.

El sector sanitario se situó algo por debajo de otros sectores, pero el *malware* distribuido a través de la nube registró un crecimiento interanual considerable, en comparación con el 30% de apenas hace un año.

El sector sanitario fue el que registró el menor porcentaje de *malware* procedente de la nube en los últimos 12 meses, por detrás de las telecomu-



nicaciones, los servicios financieros, la industria manufacturera, el comercio minorista, la tecnología, la Administración nacional y local y la educación, ocupando el sexto lugar.

Las aplicaciones en la nube son un objetivo para el *malware* cada vez más importante, ya que ofrecen a los atacantes la posibilidad de eludir los controles de seguridad habituales que utilizan herramientas como las listas de bloqueo de dominios y la supervisión del tráfico web, y estos ataques afectan a las empresas que no aplican principios de confianza cero, como los que recomienda Netskope, para inspeccionar rutinariamente el tráfico en la nube.

En Netskope se ha observado un importante cambio de tendencia en el *malware* a través de Microsoft OneDrive. Aunque Microsoft OneDrive siguió siendo la aplicación más popular en el sector, su uso fue en 2023 significativamente inferior que en otros sectores. Las descargas de *malware* a través de OneDrive fueron 12 puntos porcentuales inferiores en comparación con otras industrias. La generalización de los ataques de *malware* iniciados en OneDrive refleja la fusión de las tácticas de los adversarios (el uso abusivo de OneDrive para distribuir *malware*) y el comportamiento de las víctimas (su probabilidad de hacer clic en los enlaces y descargar el *malware*), junto con la gran popularidad de OneDrive.

Otra aplicación que ha ido ganando popularidad en el sector es Slack. Slack ocupó el segundo lugar en cargas de *malware* (por detrás de OneDrive) y el quinto en descargas, una cifra significativamente superior a la de otros sectores. Sin embargo, esta tendencia no se corresponde con el número de descargas de *malware* desde la aplicación, que ni siquiera figura entre las 10 primeras fuentes. Como Slack es una aplicación empresarial robusta, los atacantes tienen que utilizar tácticas y contenidos diferentes para dirigirse a los usuarios que han de aceptar o compartir invitaciones a canales externos. Se trata de un proceso más complejo si se compara con otras *apps* de mensajería para usuarios consumidores, como Whatsapp, que podrían utilizarse en un dispositivo de empresa. En su lugar, los atacantes emplean Slack como servidor de mando y control, ya que su API proporciona un mecanismo flexible para cargar (o extraer) datos.

Y aunque el *malware* y el robo de la información han sido los principales problemas en lo que a ciberseguridad se refiere, no pueden ser la única preocupación del sector. Es necesario ser conscientes de la vulnerabilidad de la cadena de suministro y aplicar la misma estrategia de confianza cero que aplicarían en su propia entidad si, de verdad, queremos avanzar en seguridad.



EMMA: Innovación nacional en Ciberseguridad Preventiva– más vale prevenir

Darragh Kelly
Director de Estrategia de Open Cloud Factory

Aunque vale más prevenir, ósea, ser proactivos, la realidad del modelo de ciberseguridad en el sector sanitario es reactivo. Como fabricante de ciberseguridad nacional con una gran apuesta en el sector sanitario vamos apreciando, desde hace años, un modelo reactivo con una carga, por no decir sobrecarga, de inversión en las partes de Detección y Respuesta, es decir, la seguridad que hace efecto después de que haya una incidencia, amenaza, ataque…un BANG.

Ante el crecimiento exponencial de los modelos de amenazas se puede entender la necesidad de Detección y Respuesta como clara y evidente, sin embargo, este modelo,reactivo solo no es sostenible en el tiempo. Así nos lo hacen llegar los equipos humanos quienes tienen que estar en primera línea de dichas amenazas y gestionar las soluciones reactivas.

Este modelo reactivo está orientado a **detectar más amenazas y hacerlo en menos tiempo.** El "Break out time" o Tiempo de Ruptura. Este llamado "tiempo de ruptura" es un factor crítico en el éxito de los ataques, ya que significa cuánto tiempo tienen los defensores para detectar y contener las amenazas antes de que los atacantes puedan realizar reconocimientos, establecer persistencia y localizar sus objetivos. En 2023 ese tiempo bajó a una hora, 62 minutos, 21% menos que el año anterior, a ver dónde estará el año que viene.

En lugar de progreso, encontramos fatiga con el modelo reactivo. Sabiendo que el crecimiento de amenazas y ataques crece de manera exponencial y que el tiempo que necesitan los atacantes para moverse por la red es irrisorio los equipos humanos no sienten progreso **sino fatiga** en este modo reactivo ante una realidad tan dura. El problema del modelo reactivo se agrava por la **falta de recursos y capacidades** humanas que tienen los organismos. No cuentan con el lujo de analizar los BANGs para averiguar causas raíz y realizar una mejora continua sino que están limitados a apagar fuegos y volver a prestar servicio en el menor tiempo posible con el runrún detrás de "a lo mejor esa incidencia era más de lo que parecía".

ASÍ QUE, ¿MÁS VALE PREVENIR? PARECE QUE SÍ

Debido a ello, desde Open Cloud Factory, hemos visto una tendencia y un reclamo del sector hacia la seguridad preventiva para **complementar la inversión en seguridad reactiva** con mayor foco en las partes que pasan antes que los BANGs para que los BANGs sean menos probables y menos impactantes.

Y esa es una de las grandes tendencias que hemos visto en este sector nacional y pensamos que será algo que se replicará en otros organismos. Cuando hablamos con otro organismo que no es del sector sanitario hay mucha escucha puesta ya que en sanidad se gestiona una complejidad importante además de criticalidad de los servicios, activos y datos, no podría ser mayor.
Así que, como empresa, hemos decidido doblar esfuerzos en la seguridad Preventiva en las categorías de Identificación y Protección según el Framework NIST. En los últimos años, desde la pandemia, hemos dedicado mucha inversión en I+D+i en Seguridad Preventiva.

Más información sobre Open CloudFactory escaneando el código QR:

VPN innovadora: protegiendo de manera preventiva todos los accesos a servicios centrales-usuarios internos y terceros

El coste total del VPN (cuando se tienen en cuenta los extras; 2FA, análisis de postura de *endpoints*) se ha incrementado de manera importante. Además hay organizaciones que gestionan soluciones distintas para Internos y Externos, lo que conlleva un coste de gestión adicional.

Ese incremento del coste en la tecnológica VPN en muchos casos no está reflejado en un incremento en innovación. Las soluciones tradicionales se basan en tecnología tradicional de los años 90.

"La falta de innovación y diferenciación en el mercado VPN se refleja en el hecho de que analistas como Gartner no han realizado *research* en los últimos años ni publicaciones al respecto".

OPEN CLOUD FACTORY, TECNOLOGÍA VPN MODERNA, LIGERA Y SENCILLA

Open Cloud Factory, desde la pandemia en 2020, ha invertido en su solución VPN, evolucionando sus funcionalidades y aportando más valor a sus clientes en el sector sanitario, su gran apuesta.

- Utiliza tecnología vanguardista que permite los niveles de seguridad más altos además de tener un impacto mínimo en el rendimiento.
- Cuenta con agente propio y nativo tanto para la VPN como mecanismo de analizar la postura de seguridad de los equipos como tercer criterio de permitir / denegar acceso.
- La solución cuenta con vigilancia integrada, algo innovador y único, lo que le permite al organismo monitorizar el tráfico que atraviese el túnel para que el propio túnel no se convierta en una caja negra.
- 2FA propia y integración con los mecanismos más extendidos del mercado.

¿POR QUÉ APOSTAR POR UNA SOLUCIÓN NACIONAL E INNOVADORA?

Cuenta con la confianza de ser una solución del Esquema Nacional de Seguridad (ENS) para el ENS.

EMMA-VAR (Vigilancia en Accesos Remotos) es una solución software desarrollada para el CNN-CERT por Open Cloud Factory con el objetivo de orientar a los organismos públicos en el camino de la ciberseguridad y hacia la adecuación al ENS ayudando a cumplir con 31 medidas de las 73 medidas y 24 medidas de las 54 del Perfil de Cumplimiento Específico para Salud. El producto esta certificado por el CCN-PYTEC e incluido en el Catálogo STIC 105

CON LA CONFIANZA DE ENTIDADES RECONOCIDAS

La tecnología desarrollada por Open Cloud Factory cuenta con la confianza de organismos como la Consejería de Sanidad de la Comunidad Valencia y hospitales como Consorcio Hospital General de Valencia entre otros así cómo otros organismos públicos estatales, autonómicos y europeos.

Más información:



La cuantificación del riesgo ciber como arma del CISO



Laura Prats
Cyber Risk Manager y Sébastien Jeannetot, CyberSecurity Pre-Sales specialist de Relyens en España

La gestión de los riesgos es una tarea fundamental dentro de las obligaciones de gobernanza de la Dirección de cualquier empresa, incluyendo las del ámbito sanitario. En este análisis se deben basar las **decisiones estratégicas, de inversión y operativas** de las organizaciones. Generalmente, entre los riesgos principales gestionados por la alta dirección tenemos los riesgos financieros, riesgos operativos, riesgos estratégicos o riesgos de sostenibilidad.

Los riesgos de ciberseguridad se integran principalmente en el grupo de riesgos operativos, aunque también pueden tener componentes de riesgos estratégicos y financieros. Sin embargo, hasta hace poco tiempo, estos riesgos cibernéticos no eran valorados con el nivel de atención que merecían por el equipo de alta dirección. Quedaban más o menos incluidos en un segundo nivel entre otras categorías de riesgos. Esta situación debe cambiar radicalmente, puesto que **la creciente digitalización de las empresas y su dependencia de la tecnología** exige un funcionamiento seguro para garantizar la operación de los servicios de las organizaciones. Esto, desde luego, es clave cuando hablamos de servicios sanitarios.

La inclusión de este tipo de riesgo ciber en la toma de decisión de la empresa depende de dos factores claves:

Por un lado, **la dirección debe tener formación en ciberseguridad** para comprender los riesgos que afectan al negocio, entender las soluciones para la gestión de estos riesgos y poder establecer las estrategias necesarias.

Por otro lado, deben contar con la **información adecuada para valorar correctamente el riesgo en términos empresariales.**

La necesidad de formación específica en ciberseguridad del equipo directivo es, de hecho, uno de los requisitos recogidos en el **artículo 20 de la normativa NIS 2**. Este apartado asigna a la Dirección la responsabilidad sobre el gobierno de la seguridad ciber de la compañía. En este sentido, ya se están abordando programas de formación y concienciación, pero sigue siendo preciso que esta formación incluya cómo vincular estos riesgos a la gestión de la compañía.

Adema s, es imprescindible que la información sobre los riesgos sea clara y en un lenguaje que permita tomar decisiones estratégicas y financieras. Es necesaria una **valoración económica** de los riesgos y no solo una serie de rangos cualitativos. Hasta ahora, el no tener una valoración económica ha sido una de las principales dificultades de los CISO para transmitir a la dirección el impacto de los riesgos y defender las necesidades de inversión en ciberseguridad.

METODOLOGÍAS DE ANÁLISIS DE RIESGOS: UN ENFOQUE CUANTITATIVO

Habitualmente, las metodologías más implementadas por los responsables de ciberseguridad para el análisis y gestión de los riesgos responden a otros objetivos más operativos en sus funciones: **detectar cómo las amenazas pueden impactar sobre los activos del negocio para estudiar qué medidas concretas y con qué nivel de madurez se deben implantar.** Sin embargo, la experiencia nos dice que asignar un valor económico para realizar un enfoque cuantitativo con esta aproximación, no conduce a resultados realistas desde el punto de vista del negocio.



Estas metodologías, basadas en la norma ISO 27005 (Magerit en España o EBIOS RM en Francia), son referencia para implantar Sistemas de Gestión de la Seguridad de la Información (SGSI) basados en estándares como ISO 27001 o el ENS en España. Permiten un abordaje sistemático y reproducible de los riesgos y, por lo tanto, son útiles para la toma de decisiones en la gestión operativa de la ciberseguridad, pero **no aportan información válida para los Órganos de Dirección de las empresas.**

La necesidad de un mayor enfoque económico ha hecho que el **modelo evolucione hacia metodologías como FAIR (Factor Analysis of Information Risk),** que se ha convertido en un marco fundamental para el análisis de riesgos en el ámbito de la ciberseguridad. A diferencia de las tradicionales matrices de riesgo cualitativas, FAIR ofrece un punto de vista cuantitativo que permite medir y comunicar el riesgo en términos financieros, facilitando la toma de decisiones estratégicas por parte de las organizaciones.

Esta metodología, en lugar de asignar un valor económico a los activos de la organización, lo **aplica a los servicios de negocio que sí cuentan con su propio presupuesto o ingresos.** Estos servicios se apoyan en procesos y activos tecnológicos, que son los primeros que se verán afectados en un incidente de ciberseguridad, generando unas pérdidas operacionales, reputacionales o financieras. Organismos especializados como Open Group, ISACA, NIST y COSO hacen referencia a FAIR como metodología recomendada para la gestión de riesgos ciber.

Las metodologías basadas en el estándar ISO 27005, para ser aceptadas en procesos de certificación de SGSI, deben aportar unos resultados claros y reproducibles, con una documentación estructurada que facilite la actualización de resultados y revisión de las decisiones tomadas. Además, el proceso de análisis debe basarse en la **identificación de los activos, amenazas y vulnerabilidades;** la evaluación de riesgos a través de la **probabilidad** de ocurrencia y el **impacto** generado, finalizando con el **tratamiento de los riesgos;** es decir, la selección de medidas de seguridad que, iterando el ciclo de mejora, nos lleve a un **riesgo residual.**

La metodología FAIR sigue un esquema similar, por lo que puede ser un **sistema válido para la implantación de normativa** siempre que podamos analizar el efecto de las diferentes medidas de seguridad en el cálculo de amenazas de la compañía para poder elaborar la Declaración de Aplicabilidad, basándonos en criterios de riesgo.



RELYENS CYBER CONNECT, UNA RESPUESTA ESPECIALIZADA PARA EL SECTOR SANITARIO

Desde Relyens, como expertos en la gestión de riesgos sanitarios, proponemos una solución tecnológica que aplica la metodología FAIR para la cuantificación del ciberriesgo en los entornos hospitalarios. Esta herramienta, denominada Relyens Cyber Connect (RCC), modeliza los servicios y activos del sector sanitario y su estructura de costes para calcular las posibles pérdidas en caso de ciberincidente. Además de los datos estructurales y financieros, se elabora el perfil de madurez de la ciberseguridad en base al referencial elegido por el centro sanitario.

Respecto a las amenazas consideradas, específicas para el sector sanitario, RCC se apoya en la información CTI (Cyber Threat Intelligence) proporcionada por Citalid, compañía experta en la materia. Las defensas cibernéticas se ponen a prueba mediante la aplicación de una serie de Tácticas, Técnicas y Procedimientos (TTP del marco Mitre) de las posibles amenazas identificadas para los escenarios de ataque seleccionados.

> ***La ciberseguridad es un desafío de gran calado para la digitalización del sector sanitario Es imprescindible desarrollar una estrategia correcta en la gestión de los riesgos si queremos que los servicios sanitarios cuenten con la confianza de los ciudadanos.***

Aplicando el método Montecarlo en el cálculo de riesgos y simulando los impactos de las amenazas definidas para el entorno sanitario, RCC es capaz de ofrecer un modelo de riesgos cuantitativos. Este modelo es actualizable según las mejoras en el perfil de ciberseguridad y las amenazas detectadas por el equipo de CTI. En conclusión, este análisis cualitativo apoya la tarea de la dirección para la gestión de riesgos aportando las siguientes ventajas:

- **Mejora la toma de decisiones**: permite a las organizaciones desarrollar estrategias de gestión del riesgo basadas en datos objetivos y cuantificables. La cuantificación del riesgo cibernético se establece basándose en una estructura de costes alineada con el sector.
- **Priorización de inversiones:** facilita la priorización de las inversiones en medidas de seguridad en función del impacto financiero potencial de los diferentes riesgos. Permite la elaboración y evaluación de estrategias de ciberseguridad para medir la rentabilidad de la inversión.
- **Mejora la calidad de la información y la comunicación:** agiliza la comunicación del riesgo a diferentes *stakeholders*, como la alta dirección, los equipos de seguridad y los responsables de TI.
- **Mejorar el cumplimiento normativo:** en un contexto donde las normativas sobre ciberseguridad van en aumento y son cada vez más exigentes, RCC proporciona un marco que permite su cumplimiento tanto del punto de vista del CISO como de la Dirección.

La ciberseguridad es un desafío de gran calado para la digitalización del sector sanitario. Es imprescindible desarrollar una estrategia correcta en la gestión de los riesgos si queremos que los servicios sanitarios cuenten con la confianza de los ciudadanos. Desde Relyens queremos ofrecer al sector una herramienta que sea capaz de responder a esta necesidad, teniendo en cuenta tanto el punto de vista financiero, como operativo. De esta forma, RCC se convierte en un puente entre un modelo de riesgos tecnológicos necesario para el CISO y un modelo de riesgo financiero, necesario para el CEO o Equipo Directivo.

Cumplimiento del ENS mediante el perfil de cumplimiento específico para salud



Antonio Martínez Fundador
Fundador de RIsk4all

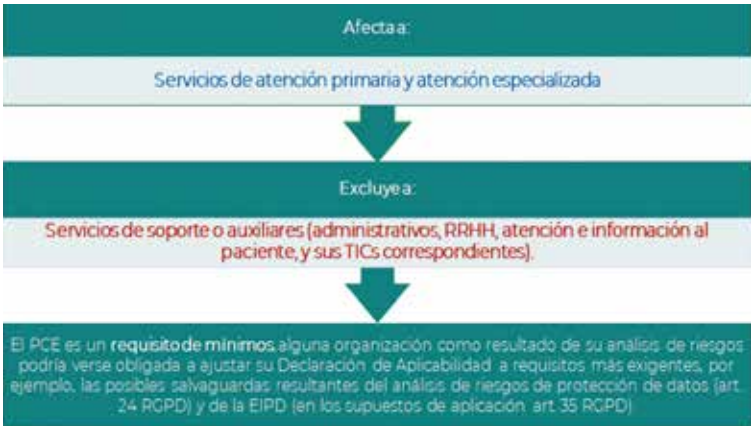
Los perfiles de cumplimiento específicos (PCE), recogidos en el artículo 30 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), son un conjunto de medidas de seguridad, que en virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS, y tras la realización de un análisis de riegos se consideran idóneas para una concreta categoría de seguridad.

A inicios de febrero se publicaba la guía CCN-STIC 891 junto a sus anexos https://www.ccn-cert.cni.es/gl/guias-es.html, guía que recoge el desarrollo del PCE para el sector salud, en concreto para los servicios e información de Atención Primaria y Atención Especializada.

Es importante recalcar que el PCE pretende alcanzar un nivel mínimo de seguridad, pero se espera que cada entidad, tras su análisis de riesgos aumente las medidas de seguridad en aquellos aspectos que resulten del análisis. También debe tenerse en cuenta que se exceptúa de este PCE otros sistemas de información para servicios de administrativos, gestión de personal, servicios de atención e información al paciente, así como tecnologías habituales o de soporte a cualquier entidad u organización.

En base a esta consideración de mínimos, se han considerado aplicables 54 de las 73 medidas de seguridad definidas en el Anexo II del ENS, no siendo aplicables las 19 que se relacionan en la figura 2.

Un total de 23 medidas de seguridad se adoptan de las requeridas para sistemas de categoría MEDIA, otras 19 para sistemas de categoría BÁSICA y 12 comunes a todas las categorías.



La guía destaca las siguientes consideraciones para algunas de las medidas de seguridad:

ANÁLISIS DE RIESGOS

En análisis debe realizarse al menos anualmente, salvo cambios relevantes de los sistemas que soportan los servicios. Se podrá utilizar cualquier herramienta con metodología clara, considerando los activos más valiosos del sistema.

Marco operacional:

[op.pl.4]	Dimensionamiento / Gestión de la capacidad.
[op.acc.3]	Segregación de funciones y tareas.
[op.exp.5]	Gestión de cabios.
[op.ext.1]	Contratación y acuerdos de nivel de servicio.
[op.ext.2]	Gestión diaria.
[op.ext.3]	Protección de la cadena de suministro.
[op.ext.4]	Interconexión de sistemas.
[op.cont.3]	Pruebas periódicas.
[op.cont.4]	Medios alternativos.

Medidas de Protección:

[mp.if.1]	Áreas separadas y con control de acceso.
[mp.if.2]	Identificación de las personas.
[mp.if.3]	Acondicionamiento de los locales.
[mp.if.7]	Registro de entrada y salida de equipamiento.
[mp.per.1]	Caracterización del puesto de trabajo.
[mp.com.4]	Separación de flujos de información en la red.
[mp.si.1]	Marcado de soportes.
[mp.si.2]	Criptografía.
[mp.info.2]	Calificación de la información.
[mp.info.4]	Sellos de tiempo.

Figura 2.

ARQUITECTURA DE SEGURIDAD

Se construirá un sistema de gestión de la seguridad, (SGSI) basado en la mejora continua, que se aplicará sobre el sistema de información que soporte los servicios en el alcance.

COMPONENTES CERTIFICADOS

Se considera relevante exigir la certificación de seguridad de los componentes a los proveedores que proporcionen sistemas y aplicaciones en este ámbito. Su aplicación a los equipos médicos probablemente requerirá de medidas compensatorias, basadas en otro tipo de certificaciones que puedan ofrecer garantías similares.

MECANISMO DE AUTENTICACIÓN PARA USUARIOS EXTERNOS

Se deberán aplicar los refuerzos R2 o R3 ó R4, mientras que para otros servicios como son la petición de cita, o similares, el acceso se podrá realizar mediante el Código de Identificación Personal (CIP) de la tarjeta sanitaria.

REGISTRO DE LA GESTIÓN DE INCIDENTES

Esta medida se orientará especialmente al aprendizaje de los incidentes registrados, con el objetivo de evitar su repetición en el tiempo.

PLAN DE CONTINUIDAD

Cada organización, en función de un Análisis de Riesgos (AA.RR.) específico que realice, podrá decidir elaborarlo, o no, ya que esta medida se ha considerado no aplicable en este PCE.

VIGILANCIA

Este servicio podrá ser prestado por un tercero, como un CERT de referencia o la Red Nacional de SOC.

BLOQUEO DE PUESTO DE TRABAJO

Se prestará especial atención a los puestos de trabajo móviles que estén ubicados en zonas públicas al alcance de pacientes, visitas, etc.

No será aplicable a equipos utilizados en los servicios de urgencia.

OTROS DISPOSITIVOS CONECTADOS A LA RED

Esta medida focalizará especialmente a los dispositivos médicos conectados a la red interna, éstos deberán estar correctamente configurados para evitar fallos o incidentes en la seguridad.

COPIAS DE SEGURIDAD

Esta medida se cetra en realizar copias de seguridad efectivas y documentadas en base a elaborar procedimientos adecuados, incluyendo frecuencia, almacenamiento. Se recomienda incluir el procedimiento de verificación para comprobar que las copias son íntegras y podrán recuperarse en el caso de necesidad.

PROTECCIÓN FRENTE A DENEGACIÓN DE SERVICIO

Se dimensionarán los componentes del sistema, especialmente los accesibles a través de Internet, con capacidad suficiente para atender con holgura la carga prevista.

Ciberseguridad y salud conectada: desafíos en cada rincón del sector sanitario



Marina Galiano
Ingeniera Ciberseguridad Industrial S2



El sector sanitario está en el punto de mira de los atacantes, convirtiéndolo en uno de los sectores más atacados del último año[1]. Pero, ¿qué debemos tener en cuenta a la hora de proteger al sector sanitario? ¿Solo son susceptibles de ataque los dispositivos médicos?

La realidad es que el sector sanitario posee varias peculiaridades que lo diferencian de otros sectores, y que deben ser tenidas en cuenta a la hora de abordar la ciberseguridad de sus sistemas como es la operación continua de sus servicios, la prioridad de la disponibilidad y la seguridad del paciente y las necesidades especiales de personal.

Por otro lado, el entorno hospitalario se caracteriza por la integración de diversas tecnologías. Además de la Tecnología de la Información (IT), se pueden identificar en tres componentes fundamentales: redes sanitarias, sistemas de gestión de edificios (BMS) y dispositivos médicos.

1 "Health theat landscape", ENISA, https://www.enisa.europa.eu/publications/health-threat-landscape

> ***La transformación digital en el sector sanitario está cambiando aún más los requisitos de ciberseguridad, lo que se traduce en una mayor complejidad, un mayor uso de dispositivos conectados y la necesidad de una nueva forma de enfocar la seguridad***

La organización sanitaria típica es un centro hospitalario con laboratorios in situ y unidades especializadas. Estas organizaciones sanitarias contienen una media de 20.000 dispositivos, incluyendo comunicaciones en sus redes médicas de dispositivos IT, IoMT, OT e IoT. Los dispositivos IT intercambian datos sensibles como registros de salud de los pacientes e información financiera, mientras que los dispositivos IoMT, OT e IoT se utilizan para una gran variedad de funciones, como la automatización de edificios, la monitorización de pacientes y la prestación de asistencia sanitaria[2].

Sin embargo, muchos dispositivos IoT en las redes de las organizaciones sanitarias no son en absoluto dispositivos médicos. Por ejemplo, sistemas de puntos de venta de las cafeterías y farmacias, máquinas expendedoras, o sistemas de edificios inteligentes para la gestión de la energía y el suministro, la climatización y los generadores de reserva.

Además, algunas instalaciones hospitalarias forman una red extendida entre el edificio principal (hospital) y sus instalaciones asociadas, como los centros de salud o los ambulatorios. Si no se tienen en cuenta las medidas de redundancia y segregación al crear esta arquitectura de red, las amenazas potenciales y los puntos de entrada para los atacantes se amplían.

Los sistemas de gestión de edificios, o BMS, se refieren a los sistemas encargados de gestionar la iluminación, el agua, la calefacción, la ventilación, etc. Es decir, los componentes de control industrial presentes en el edificio. Los BMS se incluyen en lo que se conoce ampliamente como Tecnología Operativa (OT).

Estos sistemas no están directamente conectados con los pacientes, pero son fundamentales para la prestación de la atención al paciente. Cualquier incidente que pueda afectar a estos sistemas podría tener graves consecuencias. Por ello, es de vital importancia protegerlos contra cualquier riesgo potencial, incluidas las ciberamenazas.

Cada vez existen más dispositivos médicos en las organizaciones sanitarias como consecuencia de la digitalización del sector. Hay entre 10 y 15 dispositivos médicos conectados por cada cama de paciente en los hospitales estadounidenses[3]. La transformación digital en el sector sanitario está cambiando aún más los requisitos de ciberseguridad, lo que se traduce en una mayor complejidad, un mayor uso de dispositivos conectados y la necesidad de una nueva forma de enfocar la seguridad.

Una complicación adicional de los dispositivos médicos es que la responsabilidad del mantenimiento y la protección no siempre está claramente definida, sino que suele diluirse entre diferentes departamentos. Por un lado, el departamento IT tiene conocimientos sobre medidas de ciberseguridad y sistemas de información, pero carece de información especializada sobre dispositivos médicos, como las vulnerabilidades asociadas.

Por otro lado, los ingenieros clínicos o biomédicos, que tienen un conocimiento más profundo sobre los propios dispositivos, tienen un conocimiento limitado sobre ciberseguridad. Por último, terceras partes (como proveedores o fabricantes de dispositivos) pueden tener problemas para actualizar o reparar estos sistemas por falta de permisos. Por estos motivos, los dispositivos médicos pueden caer en una zona gris que no

2 Connected Medical Device Security: A Deep Dive into Healthcare Networks," p. 29

3 "Medical devices," IBM. https://www.ibm.com/report/medical-device-security



Es crucial entender cómo está formado el sector sanitario y las tecnologías que convergen en él. Además, identificar los riesgos representa un paso fundamental hacia la fortificación de las defensas en el Sector

pertenece a ningún departamento, provocando retrasos o incluso falta de respuesta a las vulnerabilidades u otros problemas

Además, los dispositivos médicos tienen algunas problemáticas especiales, similares a las de los sistemas OT, que pueden hacerlos especialmente vulnerables a los ciberataques, y requieren una atención especial a la hora de protegerlos. De hecho, los datos muestran que hasta el 53% de los dispositivos médicos y otros dispositivos IoT conectados en los hospitales tienen una vulnerabilidad crítica conocida[4].

Las diversas regulaciones y normas que se aplican a las redes médicas, los BMS y los dispositivos médicos son vitales para las organizaciones sanitarias, ya que garantizan la seguridad de los pacientes y las instalaciones, así como el correcto funcionamiento operacional de los sistemas. Las redes sanitarias dependen de muchas normativas para su correcto funcionamiento. Las más importantes son ISO 80001, ISO 13972:2015, ISO 13485, ISO 14971, ISO 2700, ISO 27019:2017, ISO 27799, ISO 12052:2017 (DICOM) e ISO 10781:2023 (HL7). Los BMS requieren cumplir normativas similares, pero hay algunas específicas como las normas IEC 60364-7-710:2021 e ISA/IEC 62443. Los dispositivos médicos deben cumplir diferentes normativas cuando se fabrican y producen para garantizar la funcionalidad del producto, así como la seguridad del paciente. Las normas más importantes son la ISO 13485, la ISO 14971, la MDS2 (Manufacturer Disclosure Statement for Medical Device Security) y la MDR (UE 2017/745).

En conclusión, es crucial entender cómo está formado el sector sanitario y las tecnologías que convergen en él. Además, identificar los riesgos representa un paso fundamental hacia la fortificación de las defensas en el Sector. Esto es esencial para prevenir ciberataques y asegurar la integridad y la continuidad de los servicios sanitarios, no solo protegiendo así la información sino también la vida de los pacientes.

4 "53% of medical devices have a known critical vulnerability," Help Net Security, Jan. 25, 2022. https://www.helpnetsecurity.com/2022/01/25/critical-medical-device-risks/

Retos del uso secundario de los datos de salud



Gonzalo Salas Claver
Senior Manager IT Legal Advisory en SIA

En 2020, la Comisión Europea publicó la Estrategia Europea de Datos, donde se proponía la creación de espacios comunes de datos en ámbitos específicos para su uso en la economía y en la sociedad. Desde entonces, se ha avanzado de manera progresiva en diversos sectores, también en el sanitario, hasta llegar a hoy, con el Espacio Europeo de Datos Sanitarios (EEDS). En él, se abordan las singularidades que presenta la gestión de los datos de salud, tanto primarios como secundarios.

Este nuevo EEDS representa un salto cualitativo en la regulación de acceso a los datos sanitarios y un avance significativo en la interoperabilidad de los sistemas de atención sanitaria en la Unión Europea, lo que ofrece oportunidades sin precedentes para mejorar la calidad asistencial y promover la investigación biomédica. Un nuevo paradigma en el uso de los datos sanitarios a través de un modelo económico de datos que facilitará unos accesos seguros y eficientes, teniendo como clave de bóveda la capacidad de control de las personas sobre su propia información sanitaria.

Pero, para que el EEDS sea una realidad, queda mucho camino por recorrer. Va a ser imprescindible orquestar unos sistemas armonizados, interoperables, seguros, homologables y coordinados en el intercambio de datos sanitarios, donde todos los actores en juego van a tener un papel relevante. Estos son los pacientes, los profesionales médicos, las empresas proveedoras de servicios de tecnología, las Autoridades de Sanidad Digital de cada Estado y las distintas Autoridades de Control que aparecen en la ecuación (Organismos de Acceso, quienes conceden el acceso electrónico a los datos sanitarios para un uso secundario; y las Agencias de Protección de Datos, que velarán por el cumplimiento normativo sobre protección de datos).

El difícil camino por recorrer, sin embargo, va a merecer la pena. Los beneficios que se esperan son muy significativos. Para los pacientes, será posible un acceso más universal a sus propios datos de salud, lo que mejorará la atención sanitaria que recibirán por parte de los profesionales médicos, indistintamente de su ubicación geográfica. En el ámbito de la investigación, la disponibilidad de grandes conjuntos de datos acelerará los estudios y sus resultados, que permitirá una medicina mucho más personalizada que ahondará en una mejora asistencial para el paciente. Para el sector en general, la creación de un mercado único de productos y servicios sanitarios digitales dinamizará su actividad innovadora y generará empleo cualificado. Según la evaluación de impacto económico realizada, se espera que los beneficios económicos a lo largo de los siguientes diez años superen los 11.000 millones de euros frente a unos costes estimados de entre 700 y 2.000 millones.

Aun así, su implementación plantea múltiples retos en términos de protección de datos personales, interoperabilidad de los sistemas, seguridad y gobernanza de los datos, formación y desarrollo de competencias profesionales, como finalmente económicas o financieras. La participación de los espacios europeos de datos no está diseñada

bajo un modelo altruista. Los organismos de acceso a los datos sanitarios y los titulares de datos individuales podrán cobrar unas tasas[1] por el uso secundario de los mismos, que incluyan los costes relacionados con el desarrollo del procedimiento de solicitud, una compensación en concepto de una parte de los costes derivados de la recogida de los datos sanitarios.

Si bien la propuesta de Reglamento Europeo y del Consejo sobre el Espacio Europeo de Datos Sanitarios busca en este sentido establecer unas reglas con una serie de límites[2] y prohibiciones[3] en cuanto a su uso, define unos estándares e infraestructuras en un marco de gobernanza y, del mismo modo, refuerza el control del paciente sobre sus datos. A pesar de ello, se plantean una serie de cuestiones:

- Cómo materializar el consentimiento informado frente a la dificultad de garantizar que los pacientes comprendan plenamente a qué están otorgando su consentimiento, especialmente en un sistema complejo y heterogéneo. Y, también, cómo mostrar la información sobre el intercambio y uso de datos de una manera clara y comprensible, sin ningún tipo de vicio que pudiese derivar en su nulidad.



- Cómo ejecutar la interoperabilidad técnica y semántica de los sistemas, siendo necesario, para ello, la estandarización de formatos de datos, terminologías y protocolos.
- Cómo garantizar el ejercicio de los derechos de los afectados frente a unos sistemas transfronterizos y distribuidos y cómo esto se complementará con los Organismos de Acceso. Tendremos que esperar, por otro lado, para que ver qué posición acaba materializándose en esta cuestión, sobre todo, en lo que respecta al derecho de oposición: si la del Consejo de Europa, que apuesta por un modelo de exclusión voluntaria, o la del Parlamento Europeo, circunscrita al consentimiento.
- Cómo se acabarán configurando los Organismos de Acceso en un sistema descentralizado como el español.

En todo caso, estamos frente a un proyecto muy ambicioso y pieza clave de todo el sector sanitario, donde la totalidad de los actores involucrados juegan un papel significativo, que exigirá un enfoque coordinado, uniforme y conforme a la Ley, donde habrá que formarse y desarrollarse para operar correctamente en estos nuevos entornos.

1 Tasas que deben ser transparentes y proporcionadas y objetivamente justificadas y no restringirán la competencia.

2 Actividades de interés público en el ámbito de la salud pública y salud laboral, así como la protección contra amenazas transfronterizas. Apoyo a organismos públicos sanitario o asistencial. Elaboración de estadísticas al sector sanitario y asistencial. Actividades educativas en el sector sanitario o asistencia. Investigación científica. Actividades de desarrollo e innovación. Entrenamiento, prueba y evaluación de algoritmos. Prestación de asistencia sanitaria especializada.

3 Toma de decisiones perjudiciales con efectos jurídicos para una persona. Toma de decisiones para excluirlas del beneficio de un contrato de seguro o modificar sus cotizaciones y primas de seguro. Actividades publicitarias. Acceso a los datos sanitarios a terceros no mencionados en el permiso de datos. Desarrollar productos o servicios que puedan perjudicar a las personas y a las sociedades en general.

Calidad del dato en la codificación clínica ¿realmente nos importa?



Jose Ignacio Uriol Rayón
Sales Executive, Solventum, formerly 3M Health Information Systems

INTRODUCCIÓN

Estamos asistiendo a una verdadera revolución en el ámbito de la información sanitaria, donde términos como *Big Data,* inteligencia artificial, interoperabilidad, *machine learning,* ChatGPT y otros conceptos nos señalan un futuro prometedor. Sin embargo, es esencial recordar que la verdadera fuente de todos estos datos radica en la Unidad de Admisión y Documentación Clínica. Esta unidad actúa como el manantial que alimenta toda la documentación e información necesaria para aplicar las innovaciones mencionadas.

Una de las figuras esenciales es la del Técnico Superior en Documentación Sanitaria (TSDS) y la del Técnico Superior en Documentación y Administración Sanitarias (TSDAS), que se encuentran dentro de los Servicios de Admisión y Documentación Clínica (SADC), y su currículum los prepara, entre otras cosas, como los profesionales sanitarios más capacitados para construir la base de nuestra pirámide, o Sistema de Información Sanitaria. Estos profesionales, clasifican a los pacientes codificando los episodios de Hospitalización, Cirugía Mayor Ambulatoria (CMA), Urgencias (URG), Hospital de Día Médico (HDM), Consultas Externas (CEX), Lista de Espera Quirúrgica (LEQ) y el Sistema de Información del Fondo de Cohesión sanitaria (SIFCO). Desde el 2016 su principal herramienta ha sido la Clasificación Internacional de Enfermedades, 10.ª Revisión, Modificación Clínica o CIE-10-ES (Diagnósticos y Procedimientos). Pero antes hicieron uso de la 9ª revisión (CIE-9-MC) durante aproximadamente 25 años.

Esta unidad, que debería ser el manantial de información para aplicar todas las innovaciones mencionadas, enfrenta desafíos significativos. Los Técnicos Superiores en Documentación Sanitaria, quienes desempeñan un papel crucial en la calidad del dato, a veces carecen del reconocimiento y los recursos que merecen. Su experiencia se pierde con jubilaciones no reemplazadas o con la llegada de personal menos cualificado debido a la externalización del servicio. Cuanta más capacitación, y mejores herramientas se les faciliten, más fiable y explotable será la información que generan.

Con la mayor precisión que aporta CIE-10-ES, ¿cómo es posible que aún se sigan codificando determinados ámbitos con un "listado corto" o algunas LEQs con la CIE-9-MC? Ha habido Fondos Europeos hacia Hospitales y Sistemas Centrales (SSCC) para llevar a cabo grandes proyectos, TICs, desarrollos de plataformas tecnológicas, *Command Centers,* renovación de equipos, entre otros. Pero seguimos ignorando a los garantes de la calidad, que han de trabajar "mano a mano" con estas nuevas herramientas; y a los Departamentos que saben explotar estos datos para mejorar la gestión del hospital (SADC y Control de Gestión).

Otro aspecto importante a tener en cuenta, y en el que los Departamentos de Documentación también son expertos, es en la explotación y transformación de los datos en información útil para la toma de decisiones. En Estados Unidos, la codificación es el pilar fundamental para la financiación del hospital. Se auditan todos los casos para garantizar la precisión de los códigos (y, por ende, de las facturas emitidas), y se monitorizan numerosos indicadores que permiten medir la

> ***La capacidad para identificar y codificar con precisión refleja nuestro compromiso con la calidad del dato y las soluciones efectivas en el ámbito sanitario***

eficiencia, identificar prácticas deficientes y prevenir complicaciones y readmisiones (Medicare, Medicaid). En España, aunque su uso para la financiación es más limitado, siempre ha existido una cultura arraigada en el uso de estos indicadores de eficiencia y calidad como herramienta de gestión habitual. Sin embargo, algunas Comunidades no reconocen la profesión y/o no disponen de centros donde formarles. Se les exige más velocidad y que mantengan la calidad de su codificación, pero no siempre se les proporciona herramientas de ayuda. Incluso existen centros que descuidan la codificación y/o no explotan los datos que generan estos profesionales.

Pareciera que únicamente nos acordamos de ellos cuando el Hospital sale "mal en la foto" del IEMA (Índice de estancia media ajustada), cuando pierde peso relativo, o cuando la Dirección General de Sistemas de Información Sanitaria (DGSIS) de cada Comunidad Autónoma espera en tiempo y forma el fichero acumulado mensual del CMBD (Conjunto Mínimo Básico de Datos). No debemos olvidar que este CMBD ha sido la fuente primordial de información para gestionar los hospitales y será en el futuro la mejor manera de ordenar y dar continuidad a cualquier otro sistema de información mejorado que deseemos construir. Actualmente, sigue siendo el estándar de oro con el que se comparan otros sistemas de información hospitalarios, y de su calidad dependerá la calidad de la información presente en cualquier otro sistema, así como la posibilidad de validar otros sistemas de información basados en inteligencia artificial.

Últimamente se habla de preocupación y enfoque hacia el paciente, pero ¿aportamos los profesionales, los mecanismos y las herramientas para construir una pirámide de información sanitaria de calidad que permita medir si realmente estamos velando por el paciente? Decimos que el dato importa; pero, en general, no se actúa en consecuencia.

CONCLUSIÓN

En resumen, es crucial no solo conformarse con el uso adecuado de la información hospitalaria, sino extender este modelo de gestión de datos clínicos a las áreas ambulatorias, dada su creciente importancia en el panorama sanitario futuro. Aunque existen iniciativas prometedoras, como la aplicación de Inteligencia Artificial en urgencias, aún queda trabajo por hacer para integrar efectivamente la información en tiempo real en todos los flujos de trabajo y reducir la carga burocrática de los profesionales. Extender este modelo a otras áreas hospitalarias es un imperativo ético y legal, respaldado por la experiencia y los fondos disponibles, lo que subraya la necesidad de un cambio cultural en las organizaciones sanitarias para maximizar el potencial de la tecnología y el conocimiento disponibles en sistemas de información sanitaria. Este cambio, aunque requiere inversión, es fundamental para garantizar el éxito de cualquier iniciativa relacionada con los datos clínicos.

Desde Solventum, antes conocida como 3M Health Care, apostamos por este modelo de gestión de datos de calidad y colaboramos con los hospitales para la mejora de los informes, su estructuración, la calidad de lo documentado, con auditorias periódicas, y formación. Nuestro enfoque va más allá de la simple venta de herramientas; nos dedicamos a ofrecer soluciones integrales que contribuyan a alcanzar los objetivos planteados en este artículo.

Con nuestras herramientas de codificación, analizamos diariamente miles de informes hospitalarios, lo que nos confiere autoridad en la materia. En respuesta a un Responsable de Admisión y Documentación Clínica que cuestionó por qué habíamos codificado automáticamente una "implantación de prótesis de cadera en unas urgencias", la respuesta fue sencilla, "porque está documentada en el informe". Esta capacidad para identificar y codificar con precisión refleja nuestro compromiso con la calidad del dato y nuestro continuo esfuerzo por ofrecer soluciones efectivas en el ámbito sanitario.

Más allá de la consulta: la Ciberseguridad como pilar de la sanidad moderna



Aitor Aguirre (AA)
T-Systems Cybersecurity Advisor

Todo comenzó con un inocente clic en un correo electrónico que parecía provenir del departamento de TI del hospital, solicitando a los empleados verificar sus credenciales de acceso a través de un enlace adjunto. Horas después, sistemas críticos de todo el hospital comenzaron a fallar uno tras otro. Las pantallas de los ordenadores mostraban un mensaje inquietante: "Sus archivos han sido cifrados. Realice el pago en 72 horas para recuperar el acceso". El *ransomware*, introducido en el sistema a través del correo de *phishing,* había paralizado toda la infraestructura digital del hospital, desde el acceso a los registros electrónicos de los pacientes hasta los sistemas de comunicación interna, pasando por el equipamiento esencial de diagnóstico y monitorización.

> ***La protección de datos en los sistemas sanitarios se ha convertido en una prioridad, no solo para salvaguardar la información de los pacientes, sino para asegurar la continuidad y calidad del cuidado médico***

Esta historia, aunque ficticia, refleja una realidad cada vez más común en el sector de la salud: la amenaza omnipresente de los ciberataques. La irrupción de los centros hospitalarios inteligentes ha supuesto avances en el sector, pero, al mismo tiempo, los ha convertido en blanco de los '*hackers*'. Un informe de ENISA (la Agencia de Ciberseguridad de la Unión Europea) muestra que los ciberataques se duplicaron en el primer trimestre de 2023, con 40 incidentes, frente a una media de 22 en los primeros tres meses de 2021 y 2022. La propia agencia ha advertido de la importancia de proteger los hospitales por el manejo que realizan de los datos y su vulnerabilidad ante las amenazas.

La protección de datos en los sistemas sanitarios se ha convertido así en una prioridad, no solo para salvaguardar la información de los pacientes, sino para asegurar la continuidad y calidad del cuidado médico. En este artículo, exploraremos 5 estrategias críticas que las organizaciones de la salud deben implementar para blindarse ante posibles ciberataques. Las principales amenazas de ciberseguridad que impactan en el sector son:

1. Ataques de Ransomware: El *ransomware* representa una grave amenaza para las organizaciones de atención médica, ya que puede interrumpir las operaciones y comprometer la



atención al paciente. Para detectar amenazas de *ransomware*, es crucial implementar sistemas de detección de intrusiones robustos y realizar evaluaciones periódicas de vulnerabilidad.

2. Violaciones de Datos: El robo de registros de pacientes conlleva violaciones de privacidad y daño a la reputación. La implementación de protocolos de cifrado para datos en movimiento y en reposo puede prevenir el acceso no autorizado. Asimismo, la vigilancia continua y el registro de actividades en red facilitan la detección temprana de brechas de seguridad.

3. *Phishing* e Ingeniería Social: Los correos electrónicos de *phishing* y las tácticas de ingeniería social siguen siendo los métodos predominantes para obtener acceso no autorizado a los sistemas de atención médica. Los programas de capacitación centrados en identificar intentos de *phishing* y verificar la autenticidad de las solicitudes pueden reducir significativamente este riesgo.

4. Vulnerabilidades de la Cadena de Suministro: Las organizaciones de atención médica a menudo dependen de proveedores externos para diversos servicios y productos, lo que puede introducir vulnerabilidades de seguridad. Realizar evaluaciones exhaustivas de riesgos y establecer requisitos de seguridad estrictos dentro de los contratos son elementos esenciales para reducir amenazas.

5. Explotación de Dispositivos IoMT: La proliferación de dispositivos de Internet de las cosas en el ámbito de la salud presenta nuevas superficies de ataque. Es fundamental que las organizaciones segmenten los dispositivos IoMT de las redes críticas, actualicen regularmente el *firmware* del dispositivo y utilicen soluciones de monitorización de redes para detectar comportamientos anómalos.

Para protegerse frente estas vulnerabilidades, es recomendable considerar cinco áreas o dominios de actividad dentro de la gestión del riesgo:

1. Identificación: Estas medidas de ciberseguridad se basan en detectar posibles amenazas o vulnerabilidades dentro de los sistemas informáticos y las redes de una organización. Estas estrategias suelen apoyarse en tecnologías avanzadas y procedimientos específicos para identificar actividades anómalas o potencialmente maliciosas.

2. Protección: Las estrategias de protección ayudan a anticiparse y reforzar la protección



de los ataques. Incluyen la implementación de marcos robustos de ciberseguridad, el uso de autenticación multifactorial, la actualización regular de software y parches, y la realización de capacitación periódica en conciencia de seguridad para los empleados.

3. Detección: La detección temprana permite ofrecer una respuesta ágil y contundente. Esta estrategia. Esta estrategia se basa en la monitorización continua del tráfico de red, la implementación de sistemas de detección de intrusiones y el uso de análisis de comportamiento para identificar actividades sospechosas.

4. Planificación Un plan de respuesta a incidentes bien definido es crucial para contrarrestar amenazas de forma rápida y efectiva. Este plan debe incluir procedimientos para contener incidentes, preservar evidencia, notificar a las partes interesadas y restaurar los sistemas a la operación normal.

5. Recuperación: Es, sin duda alguna, un punto clave de protección. La estrategia de recuperación posterior implica contar con soluciones que permitan restaurar datos: desde realizar copias de seguridad, a análisis forenses para determinar la causa raíz del incidente, e implementar medidas para prevenir incidentes en el futuro.

En el nuevo paradigma digital de hoy, donde la línea entre la tecnología y la atención médica se vuelve cada vez más difusa, la ciberseguridad no es solo una opción, sino una necesidad imperativa. La pregunta que cada institución debe hacerse no es si ocurrirá un ciberataque, sino cuándo ocurrirá y si estará preparada para responder.

Por tanto, la ciberseguridad en el sector de la salud no es solo responsabilidad de los equipos de TI; es una misión crítica que requiere el compromiso de todos los niveles de la organización, desde la junta directiva hasta el personal clínico y administrativo. Al adoptar un enfoque proactivo y colaborativo, las organizaciones de atención médica no solo pueden defenderse contra las ciberamenazas, sino asegurar un entorno en el que la atención al paciente pueda prosperar sin interrupciones. Como dice el dicho, "más vale prevenir que curar". Y con ello ganamos todos, reforzamos las defensas de los sistemas, pero también la seguridad de los pacientes y la integridad de la institución dependen de ello.

XXI REUNIÓN DEL FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD

La XXI Edición del Foro de Seguridad y Protección de Datos de Salud de la SEIS tuvo lugar en Toledo los días 14 y 15 de febrero del 2024 y giró sobre uno de los retos candentes en materia de protección de datos y seguridad como es la utilización de los datos de salud, tanto en el uso primario como secundario que se presenta en áreas como la atención o la investigación sanitaria.

TOLEDO, JUEVES 15 DE FEBRERO DE 2024
"RETOS Y LÍMITES DEL USO DE LOS DATOS DE SALUD"

ACTO DE INAUGURACIÓN



La inauguración contó con las intervenciones de **Jesús Fernández Sanz,** consejero de Sanidad del Gobierno de Castilla La Mancha; **Juan Fernando Muñoz Montalvo,** secretario general de Salud Digital, Información e Innovación en el Sistema Nacional de Salud del Ministerio de Sanidad; **Luciano Sáez Ayerra,** presidente de la Sociedad Española de Informática de la Salud; **Mar España Martí,** directora de la Agencia Española de Protección de Datos; y **Sagrario de la Azuela Gómez,** directora-gerente del Complejo Hospitalario Universitario de Toledo.

El presidente de la SEIS, **Luciano Sáez**, tras los agradecimientos a los asistentes, organizadores y patrocinadores, quiso dedicar unas palabras al Servicio de Salud de Castilla-La Mancha, reconociendo que "ha dado un gran salto" con el objetivo de servir de encuentro del sector para ayudar a implantar medidas de seguridad de los SSII y sus datos, así como servir de canal de comunicación a las propias autoridades de protección de datos. También recordó que, en 2013, se constituyó en el seno de esta sociedad el Comité Técnico de Seguridad de SSII de Salud, compuesto por todos los responsables de seguridad y protección de datos de los servicios de salud, siendo Juan Díez su coordinador.

Sagrario de la Azuela tuvo una breve intervención en la que, además de realizar agradecimien-

tos, afirmó que la asistencia sanitaria, de por sí una tarea compleja, "ahora está en constante riesgo de terrorismo cibernético" que "obliga a estar en guardia".

Juan Fernando Muñoz Montalvo, por su parte, señaló que "uno de los tangibles más importantes que tiene el SNS es la confianza en sus datos, por lo que debemos protegerlos". Informó que en pocos meses estará aprobado el reglamento del Espacio Europeo de Datos de Salud y afirmó que en intercambio de datos primarios –información clínica– España ya es líder porque "tenemos once CC AA con intercambio pleno de la HC resumida europea y trece de la receta electrónica", faltando especialmente la parte privada y el mutualismo. En cuanto al uso secundario de datos, el reglamento "supone un cambio muy importante" con "unas condiciones de equilibrio" que permitirá la condición sin necesidad del consentimiento informado, siempre de forma anonimizada o, en excepciones, pseudoanonimizada, existiendo prohibiciones claras.

También destacó el proyecto colaborativo que supone el Plan del Transformación de Atención Primaria y Salud Comunitaria, con un grupo de trabajo sobre seguridad cooperativo entre las CC AA liderado por Baleares.

A continuación, intervino Mar España Martí, directora de la Agencia Española de Protección de Datos, quien quiso empezar recordando el "compromiso pleno de la Agencia en garantizar la privacidad de los datos, intentando flexibilizar al máximo", en el marco de un modelo competencial "donde tenemos que ir todos de la mano" asegurando que "es un proyecto de país". También calificó de "salto importante" la iniciativa de la UE para regular la Inteligencia Artificial, asegurando que es importante que establezca también los criterios de protección y clasificación de los riesgos.

Por último, intervino el consejero, Jesús Fernández Sanz, quien aseguró que "en Castilla-La Mancha trabajamos de manera incansable en la protección de los datos", señalando que hace unos años el origen de los datos estaba acotado al acto clínico y el papel, pero ahora está diversificado y tiene un espacio mucho más amplio". También calificó como "reto más importante" el uso primario y, sobre todo, el uso secundario de los datos para investigación y salud pública.

PRIMERA SESIÓN



La primera sesión estuvo moderada por Juan Ángel Morejudo Flores, viceconsejero de Transformación Digital de la JCCM, y contó como autoridades en protección de datos con Mar España Martí, directora de la Agencia Española de Protección de Datos; Meritxell Borràs i Solé, directora de la Autoridad Catalana de Protección de Datos; Unai Aberasturi Gorri, director de la Agencia Vasca de Protección de Datos; y Jesús Jiménez López, director del Consejo de Transparencia y Protección de Datos de Andalucía.

El moderador, tras señalar que hay que lograr un equilibrio entre servicio al ciudadano con uso de la tecnología y la garantía de protección de datos, dio paso a la intervención de cada uno.

La directora de la Agencia Española de Protección de Datos, Mar España, comenzó su intervención con un llamamiento por la nueva ley de *protección infantil* que el Gobierno del Estado acababa de anunciar, para que, ante el creciente impacto en la salud mental en los menores por el abuso en el uso de la digitalización, se aporten propuestas para incluir en el futuro protocolo de prevención del menor al consumo abusivo de lo digital.

A continuación, expuso que hay un deseo de "ser los primeros" en regular sobre *neuroderechos*, ante el hecho de que con las nuevas interfaces con el cerebro ya no solo "se puede descodificar actos conscientes e inconscientes sino que también se puede modificarlos", lo que va a permitir "maravillas", como que parapléjicos hablen, pero también que las empresas de dispositivos cerebrales vendan luego datos de las mentes de las personas: son los "neurodatos", que, "por supuesto, son datos personales", "extremadamente privados", que hay que proteger de forma especial.

Por su parte, la directora de la Autoridad Catalana de Protección de Datos [APDCAT], Meritxell Borràs, coincidió en que estamos entrando en la revolución industrial 5.0, la de la simbiosis entre humanos y máquinas, y continuó explicando que el Plan Estratégico de la PDCAT se ha realizado "teniendo claro que las personas son el centro de nuestras atenciones" si bien "ningún derecho es absoluto". Reconoció que el "mayor reto ahora" es el uso de la *IA*, apuntando como sus riesgos la toma de decisiones sesgada, la falta de transparencia de algoritmos, la pérdida de empleos y los sistemas mal diseñados e, incluso, diseñados para usos maliciosos.

Así, la autoridad catalana "diversifica sus actuaciones"; entre ellas, citó una guía de salud vinculada al nuevo espacio europeo de datos de salud [EEDS] o la creación de una red de delegados de Protección de Datos (no solo de salud) que tiene carácter transversal y tiene ya más de 200 miembros, con el objetivo de intercambiar conocimiento, compartir recursos, facilitar formación, formar grupos de trabajo, foros de debate, etc.

En su turno, el director de la Agencia Vasca de Protección de Datos, Unai Aberasturi, comentó que el ámbito sanitario es especialmente complejo, también en aspectos jurídicos de la protección de datos por los diferentes tipos de uso de datos y de perfiles de usuarios y una tecnología que "avanza a velocidad vertiginosa". Informó que en diciembre de 2023 se ha aprobado una modificación de la Ley Vasca de Protección de Datos para ampliar su ámbito –en Sanidad del Servicio Vasco de Salud a todo el sector público vasco–. Apeló a "aumentar la colaboración y cooperación entre autoridades desde el principio" y finalizó lanzando preguntas: ante reclamaciones que llegan de ciudadanos pidiendo que sus datos no acaben en el EEDS, ¿es necesario consentimiento? y ¿qué recorrido tiene allí el ejercicio de una oposición al acceso?

> ***Hay un deseo de "ser los primeros" en regular sobre neuroderechos, ante el hecho de que con las nuevas interfaces con el cerebro ya no solo "se puede descodificar actos conscientes e inconscientes sino que también se puede modificarlos", lo que va a permitir "maravillas", como que parapléjicos hablen, pero también que las empresas de dispositivos cerebrales vendan luego datos de las mentes de las personas***

Jesús Jiménez López, director del Consejo de Transparencia y Protección de Datos de Andalucía, señaló que cualquiera que sea la tecnología siempre va a tener superpuesta la protección de datos: siempre habrá una normativa que cumplir. Así, afirmó que "vamos a exigir el cumplimiento de la normativa específica de la IA en cuanto a Protección de Datos". Sobre transparencia, indicó que ya hay un consenso en cuanto a los datos genéricos, pero "no se tiene idea" de lo que se está haciendo con los genómicos, donde hace falta transparencia en sus usos.

En cuanto a la IA, reconoció que la mayor dificultad está en identificar quién es el responsable y quién es el encargado del tratamiento de los datos. Finalizó señalando que "tenemos que trabajar de una forma más homogénea y con un lenguaje común".

SEGUNDA SESIÓN: SOLUCIONES PARA LA CIBERSEGURIDAD EN ENTORNOS SANITARIOS



La segunda sesión fue presentada por **Jesús Manuel Carrasco Raso,** responsable de la Unidad de Ciberseguridad de la Dirección de Salud Digital del Servicio de Salud de Castilla La Mancha, quien comentó algunos proyectos del SESCAM: un SOC en colaboración con el CCN-CERT adherido a la red nacional de SOC y la monitorización de dispositivos médicos mediante sondas.

La sesión estuvo compuesta por tres conferencias dictadas por autoridades en el mundo de la ciberseguridad.

La primera conferencia fue a cargo de **José Serrano,** miembro del Área de Normativa y Servicios de Ciberseguridad del Centro Criptológico Nacional. Aseguró que "no hay transformación digital sin ciberseguridad", por lo que es imprescindible una estrategia y una gobernanza de la ciberseguridad, señalando que la ciberamenaza ha cambiado a grupos de ataques coordinados, profesionalizados y especializados, por ejemplo, en blanqueo de capitales. También ha crecido "enormemente" el mercado de servicios, citando algunos tipos de soluciones para varios tipos de ataques: para la suplantación de identidad, el doble factor, para los ataques a los dispositivos médicos, su gestión y seguridad por diseño... Comentó que a los autores de los ciberataques "no les pasa nada si fracasan", con lo que no hay disuasión, siendo conveniente un mayor marco regulatorio.

En opinión de José Serrano, hay que adaptar una postura de seguridad realista y, en general, intentar aplicar el ENS basándose en tres pilares: diagnóstico, adaptación al medio y mejora continua. Se están lanzando perfiles de cumplimiento específicos o PCE para sectores de actividad. Así se ha publicado el PCE para Salud en el CCN-STIC891, que contiene una lista amplia de medidas, algunas específicas del sector.

Después, **Juan Diez González,** responsable de ciberseguridad para sectores estratégicos Sanitario, Alimentario y de Investigación de INCIBE, dedicó su conferencia a las amenazas en el sector de Salud, afirmando que ya es el segundo sector más atacado. Recordó que el INCIBE-CERT es el CSIRT nacional para los ciudadanos, pymes y sectores estratégicos privados, mientras que, para lo público, está el CCN-CERT. Señaló que la normativa actual no obliga al sector privado a informar de incidentes de seguridad. De hecho, el año pasado no se recibió comunicación de ningún incidente del sector salud, cuando debió haber muchos y, varios, importantes.

Pero, en enero de 2023, se publicó la NIS2, que cuenta entre sus cambios principales la obligación de comunicar incidentes también al sector privado, permitiendo además deshabilitar a gestores que no cumplan con esa obligación, incluyendo un régimen sancionador. Como recomendaciones, citó contar con una estrategia en colaboración y una planificación ante desastres.

La última conferencia corrió a cargo de **Leandro Gobierno López,** responsable para la elaboración de normas, estrategias e iniciativas de ciberseguridad y cibercriminalidad de la Oficina de Coordinación de Ciberseguridad (OCC) del Ministerio del Interior, quien comenzó explicando que la OCC trabaja bajo estos principios: los ciberincidentes son en su mayoría ciberdelitos, hay que dotar de seguridad tanto física como digital de manera coordinada y hacer un balance entre prevención y respuesta. Comentó que es la autoridad para los operadores de servicios críticos esenciales, sirve de enlace entre los CSIRT y el CCN y coordina la implementación de NIS2 en los sectores, elaborando guías. Se estructura en dos divisiones: una de operaciones e incidentes y otra de planificación y estrategia.

Tras opinar que el sector sanitario privado, con sus 117.000 empresas, se "enfrentan ante un reto", siendo creciente la relevancia de ciberseguridad, realizó un repaso de aspectos de seguridad de algunas tecnologías:

- servicios a la nube: los proveedores son ajenos a la UE y se exige que sus CPDs estén en la UE.
- IA y analítica de datos: el dato de salud es especial, como también debe ser su protección
- IoT: la OCC ha publicado una guía.
- Robotización: sector "muy goloso" para ataques.

TERCERA SESIÓN: RETOS PARA EL USO SECUNDARIO DE DATOS DE SALUD



Esta tercera sesión estuvo moderada por **Manuel González Seco,** de la Jefatura del Gabinete de Cumplimiento de Transparencia y Protección de Datos de Andalucía, y contó como participantes con **Jesús Rubí Navarre**, vocal coordinador de la Unidad de Apoyo y Relaciones Institucionales de la Agencia Española de Protección de Datos; **Lucía Escapa Castro**, jefe del Gabinete del Secretario General de Salud Digital, Información e Innovación para el Sistema Nacional de Salud del Ministerio de Sanidad; **Carlos Luis Parra Calderón**, jefe de Sección de Innovación Tecnológica del Hospital Universitario Virgen del Rocío; **José Luis Rojo de Luque,** socio de Technology Consulting de EY, y **Gonzalo Salas Claver,** senior manager de IT Legal Advisory en SIA.

Así, **Carlos Luis Parra**, preguntado por los retos en uso secundario para investigación, señaló que, en este ámbito, mientras está "demostrada la necesidad de hacer uso de datos de salud y además cada vez a más escala", a la comunidad científica "le cuesta creer en la privacidad", siendo el principal reto, por tanto, el de "resultar confiables para los proveedores sanitarios".

Por su parte, **Lucía Escapa,** preguntada por las limitaciones del Reglamento del Espacio Europeo de Datos de Salud, apuntó que, en origen, el

reglamento surgió con la idea de poder reutilizar los datos de salud sin necesidad de consentimiento informado para las excepciones del uso secundario: en general, innovación, investigación y docencia, y ya solo para la AAPP, la salud pública, políticas públicas y estadísticas, contemplando el reglamento la prohibición expresa de los usos para perjudicar a terceros, marketing y seguros. También obliga a todos los proveedores a publicar sus catálogos de datos. Y no se permite acceder, para esos usos secundarios, a datos de salud identificados.

El moderador preguntó a **Jesús Rubí** cómo afectaba este reglamento al consentimiento y a la pseudoanonimización. Respondió que se modifica la normativa del consentimiento al levantarse una prohibición; ahora el consentimiento es más amplio en casos de investigación. Y para la pseudoanonimización se exige separación técnica entre quien la realiza y la investigación, que usará los datos pseudoanonimizados. Aseguró que el "nuevo marco va a permitir la investigación sanitaria".

Gonzalo Salas, preguntado por la situación en qué queda el ciudadano, afirmó que se le "generan muchas incertidumbres", siendo "importante que haya controles de acceso y transparencia" así como una posibilidad de ejercicio de oposición al acceso.

José Luis Rojo contestó afirmativamente a la cuestión de si existen riesgo sistémico: "sin duda, al estar muchas organizaciones interconectadas".

En una ronda de opiniones libres, **Gonzalo Salas** reconoció que, con el reglamento, se plantea un modelo completo a la hora de compatibilizar el uso secundario de datos con la protección de datos; Carlos Luis Parra señaló que la gestión del acceso a datos a veces agota tanto al científico que "ya no le quedan ganas de investigar". Lucía Escapa afirmó, por su parte, que "como país estamos en una posición de privilegio para implantar este reglamento europeo.

CUARTA SESIÓN: SOLUCIONES DE CIBERSEGURIDAD Y GESTIÓN DE RIESGOS



La cuarta sesión fue presentada por **Pol Pérez i Sust,** director del Área de Sistemas de Información del Servei Català de la Salut (CatSalut) y coordinador general de las TIC del Departament de Salut de la Generalitat de Catalunya, quien reconoció que "en nuestras instituciones hay muchos puntos de ataque, son centros muy porosos", en las que se da no solo secuestro de datos vía *ransomwares* sino también robo y venta de datos en la *deepweb*, como sucedió en el caso del H. Clinic.

La primera intervención fue de **Ferrán Orsola**, principal sales engineer para EMEA de **Gigamon,** quien expuso su solución de visibilidad de todo el tráfico de la red, mediante duplicaciones con dispositivos TAP en todas las conexiones. La calificó de "el *big brother* de la red". La primera experiencia en sanidad pública a

nivel regional ha sido en Baleares, habiendo conseguido recientemente el contrato de una CC AA con 3,5 hospitales.

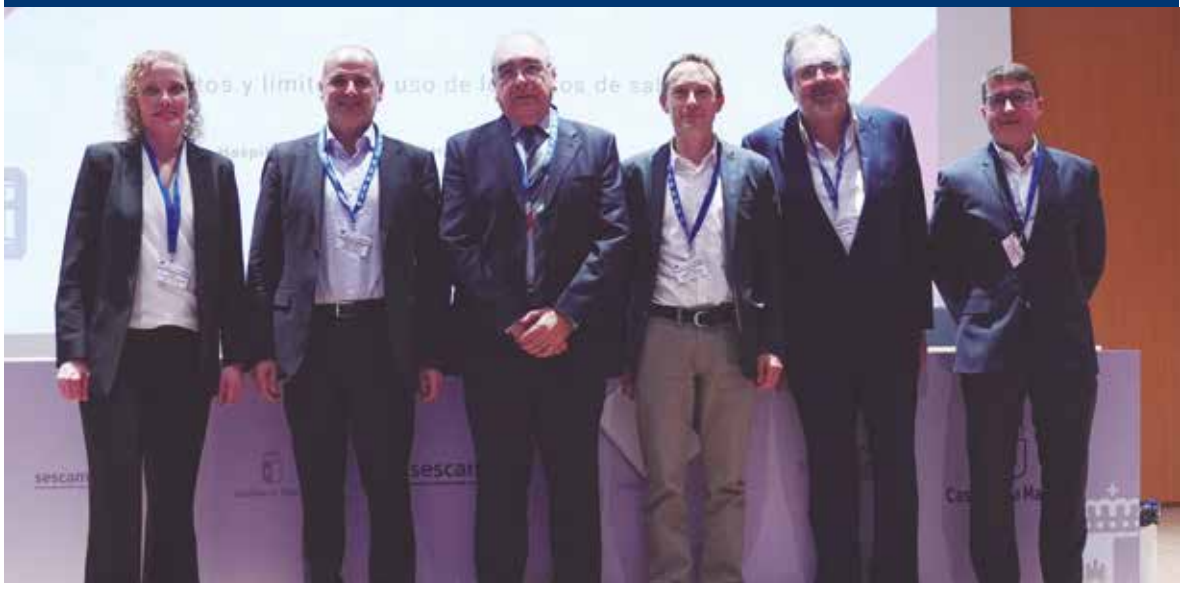
A continuación, José **Antonio Sánchez Ahumada,** *sales director* Spain and Portugal de **Claroty-Medigate**, realizó un símil entre hospitales y ciudades en cuanto a sus retos comunes, concluyendo que "si homogeneizamos seremos más eficientes", en ambos casos, también en las redes de TI de un hospital.

Por su parte, **Miguel Ballesteros,** director del Centro de Competencia en Ciberseguridad de **Oesia,** comenzó con la pregunta "¿estás seguro de todo lo que tienes conectado?", para a continuación exponer su solución global EMMA, que identifica el inventario de dispositivo conectados y los riesgos que tenemos con él, además de proveer una sonda y herramientas de segmentación y enmascaramiento de vulnerabilidades.

Antonio Martínez, fundador de la herramienta **Risk4all,** recordó que hay un perfil de cumplimiento específico [PEC] del ENS para salud recientemente publicado, siendo Risk4All una herramienta que evalúa el cumplimiento de las diferentes medidas del PEC –como arquitectura de seguridad, inventario de dispositivos conectados, componentes certificados, mecanismos de autentificación, registro de incidentes, plan de continuidad, copias de seguridad, etc– y genera un informe.

Por último, **Javier López,** *healthcare account executive* de **T-Systems,** realizó la presentación "La relevancia del back up inmutable en el entorno salud", comentado su solución Exagrid, que permite tener dos zonas: una visible en la red y otra oculta a la red, inmutable y con deduplicación.

QUINTA SESIÓN: RETOS EN LA VALIDACIÓN DE LOS ALGORITMOS PARA EL DIAGNÓSTICO Y TRATAMIENTO MÉDICO



Esta quinta sesión estuvo moderada por **Francesc Xavier Urios Aparisi,** jefe de la Asesoría Jurídica de la Autoridad Catalana de Protección de Datos, y contó como participantes con **Juan Díaz García,** coordinador del Comité Técnico de Seguridad y Protección de Datos de la SEIS; **Amador Ruiz Torrejón,** coordinador autonómico de Sistemas de Información Clínico del Servicio de Salud de las Illes Balears; **Joaquín Cañada González,** delegado de Protección de Datos de la Comunidad Valenciana; **Marcial García Rojo,** director de la UGC Anatomía Patológica del Hospital Universitario de Jerez; y **Diana de la Iglesia Jiménez,** directora de Desarrollo de Negocio de Genómica, Inteligencia Artificial y Analítica Avanzada en Fujitsu.

Juan Díaz señaló que los sistemas de IA están ya presentes en los comités de contratación, éticos, etc., pero se preguntó cuántos han pasado por la

Agencia Española del Medicamento y han sido validados como producto sanitario europeo: ninguno.

Por su parte, Amador Ruiz, confesó que, como clínico, "me preocupa de dónde saca la IA las conclusiones sobre los datos". Joaquín Cañada coincidió y habló de la necesidad de transparencia algorítmica, para lo que en la Comunidad Valenciana se había decidido aprobar un registro de algoritmos, así como de la conveniencia de la aplicabilidad de los algoritmos.

Marcial García Rojo afirmó que los algoritmos de IA están "funcionando muy bien" en patología, citando como retos: el acceso a la propia tecnología, la necesidad de estandarización de procedimientos e interoperabilidad –señalando la falta de anotaciones en el suplemento 145 de DICOM para Patología Digital– y la validación de los algoritmos que desarrollamos en hospitales.

Diana de la Iglesia señaló algunos aspectos clave: la disponibilidad de los datos, "la tecnología no es neutra" y para validar algoritmos es necesaria la intervención humana.

El moderador preguntó por el papel que debe tener la IA para la toma decisiones médicas. Amador Ruiz respondió con otra pregunta: "¿quién se va a sentar en el banquillo cuando haya malas decisiones médicas de la IA? Diana de la Iglesia matizó que la idea actual no es que la IA decida, sino que sea "una especie de copiloto".

También preguntó el moderador por los posibles *sesgos,* reconociendo Amador Ruiz que hay más sistemas entrenados con pacientes de EEUU–donde es más fácil conseguir sus datos-. Marcial señaló que además los algoritmos no son buenos si hay poca prevalencia y para el caso de la genómica en la UE, entre el 70 y el 80% de los datos accesibles son de población europea, con lo que las conclusiones solo valen para europeos.

SEXTA SESIÓN: CASOS PRÁCTICOS: LA EXPERIENCIA DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS



El moderador, Pedro Alberto González, exresponsable del Registro y Auditoría de Ficheros de la Agencia Vasca de Protección de Datos, comenzó dando las gracias a la organización, asistentes y autoridades, para seguidamente presentar a las ponentes. A continuación, indicó los principios en los que se centrarían los casos expuestos.

Licitud, lealtad y transparencia

María Isabel Navarro Alonso, vocal asesora de Inspección de Datos de la Agencia Española de Protección de Datos, expuso que la reclamación del Formulario de Control Sanitario de entrada en puesto y aeropuertos de Baleares con motivo de la COVID-19 no cumplía las exigencias del art. 13 del RGPD, ya que no concretaba la base de legitimación ni los motivos en los que se amparaba la recogida de datos de salud. Además, la normativa recogida no estaba vigente en el momento de los hechos. Se sancionó al responsable público con apercibimiento, debido a que no se informaba de forma correcta.

Minimización de datos

En primer lugar, Juana Vegas Fernández, letrada instructora de la Asesoría Jurídica de la Agencia Vasca de Protección de Datos, expuso la reclamación de un matrimonio que se separa y surge el problema con la custodia de los hijos. La esposa solicita si el marido está en un tratamiento de adicción a las drogas para reclamar la custodia, el Servicio Vasco de Salud le envía toda la historia clínica desde 2000 a 2018, incluyendo toda la información no solicitada. El marido reclamó al Juzgado que se le dio más información de la que solicitaba. Se apercibió al Servicio Vasco de Salud por vulneración del principio de minimización y se le requirió que tomase las medidas organizativas internas para evitar situaciones como las referidas en el futuro.

Seguidamente, Nuria Pedros Ramos, autoridad catalana de la Agencia de Protección de Datos, expuso el caso de una entidad que publicó en su página web el listado de personas admitidas y excluidas en un proceso de selección, incluyendo a las personas con discapacidad y su grado. Se sancionó a la entidad, que presentará recurso contencioso administrativo contra esta sanción.

También se mencionó el caso de que un consorcio sanitario fue denunciado por enviar la historia clínica completa de un paciente a un juzgado que solo solicitaba un episodio concreto. Se dio la razón al denunciante.

Otro caso en el que un hospital público solicitaba el nombre, apellidos y DNI para identificar a la persona que llamaba y se consideró que no era excesivo, ya que se consideró que era necesario para verificar que la persona que llamaba era quién decía ser.

Exactitud y vigencia

En primer lugar, Juana Vegas Fernández expuso el caso de un paciente al que no le llegaban las comunicaciones del hospital, porque su domicilio era inexacto. La denuncia fue porque no pudo acceder a las campañas de cáncer de colon ni de cáncer de mama de forma precoz y resultó que se le detectó un cáncer de mama posteriormente. Se decidió apercibir al Servicio Vasco de Salud, pero el caso ha generado una reclamación patrimonial.

Otro caso el de un paciente en cuya historia clínica no ponía que era diabético y alérgico al nolotil. En un accidente se le suministró nolotil y la reacción la pudieron coger a tiempo porque estaba en el hospital.

A continuación, Nuria Pedros Ramos expuso el caso de un denunciante que exponía que, a raíz de una discusión con la administrativa de un centro de atención primaria, se accedió a su historial clínico indebidamente para modificar su correo electrónico. El denunciante recibió una llamada anónima, y la entidad denunciada investigó el caso y consideró que se había producido un acceso indebido y una falta, ya que se cambió el correo electrónico sin justificación ni consentimiento. Se resolvió que la entidad había vulnerado el principio de exactitud y el de confidencialidad.

Integridad y confidencialidad

En primer lugar, Blanca Álvarez Yagüe, responsable del Área de Protección de Datos del Consejo de Transparencia y Protección de Datos de Andalucía, expuso el caso de un acceso indebido a la historia clínica por parte de profesionales sanitarios de otros países de la UE. La entidad indica que la plataforma solo daría acceso en caso de que el paciente necesitara asistencia en algún otro país, por tanto, el consentimiento no sería necesario. Esta denuncia formaba parte de la campaña orquestada por redes sociales.

También abordó el caso en que unos hijos denunciaron que se había dado información a la pareja de hecho de su padre sin su consentimiento. Al estar el padre en coma, no pudo dar su consentimiento, pero la Ley de Autonomía del Paciente indica que también se podrá dar información a personas vinculadas por razón de hecho o de derecho. Por tanto, la denuncia se desestimó por considerarse que estaba vinculada por razón de hecho.

A continuación, María Isabel Navarro Alonso expuso el caso en el que un denunciante puso de manifiesto que se habían realizado accesos indebidos a su historia clínica. Tras la investigación interna que realizó el responsable del tratamiento, se consideró que todo era correcto, pero el denunciante solicitó el informe de la auditoría y al recibir el listado con los accesos consideró que había accesos no justificados por parte de dos compañeros. Se impusieron dos sanciones de apercibimiento a la responsable del tratamiento y se propuso el inicio de actuaciones disciplinarias.

Seguidamente, Juana Vegas Fernández expuso el caso de un habitante de un pueblo al que sus vecinos preguntaban continuamente por su salud. Resultaba que una sobrina suya con la que no tenía buena relación trabajaba en el Centro de Salud. Se puso una denuncia, pero tras la investigación, quedó acreditado que la sobrina nunca había accedido a la historia clínica del reclamante y se archivó el expediente.

Finalmente, Nuria Pedros Ramos expuso el caso de un paciente que denunciaba que se había accedido a su historia clínica desde un Centro de Salud, en el que había presentado varias denuncias sin obtener respuesta. Tras la investigación se detectó que la persona que había realizado los accesos fue el delegado de Protección de Datos en el ejercicio de sus funciones, ya que debía dar respuesta a otras reclamaciones interpuestas por el denunciante. Por tanto, la denuncia fue archivada.

Responsabilidad proactiva

En primer lugar, María Isabel Navarro Alonso expuso el caso en el que se inician actuaciones por propia iniciativa de la directora de la AEPD, que insta a la SGI al inicio de actuaciones para comprobar si se cumple lo establecido en el Decreto 29/2009 que regula el uso y acceso a la historia clínica electrónica, sobre los módulos de especial custodia. El responsable del tratamiento explicó que se había unificado toda la información del paciente de estos módulos a través del módulo de acceso general que requiere usuario y contraseña, además de necesitar un permiso adicional para acceder. Se archivó al considerarse que las medidas de seguridad eran adecuadas.

A continuación, expuso el caso de un médico que denunció que se le había metido en un grupo de Whatsapp sin su consentimiento, en el que además se trataban datos médicos. El responsable de la entidad dice que lo conoce, que solo es profesional y que se incluyen otros profesionales con convenio, para consultas internas. Se investigó si se podía haber producido algún incumplimiento, y se decidió que el del consentimiento para agregar al denunciante al grupo de Whatsapp sí. En cuanto al tratamiento de datos, se consideró legítimo el uso en el grupo, pero como no se tenía consentimiento de los pacientes, ni la finalidad era la correcta y Whatsapp no cumple con las medidas de seguridad adecuadas, se decidió cerrar todos estos grupos, ya que además la organización tenía herramienta corporativa que sí cumplía con los requerimientos de seguridad.

También expuso el caso en el que la Consejería habilitó vía web la posibilidad de que los ciudadanos obtuvieran el Certificado COVID Digital, pero, debido a un fallo en el procedimiento de autenticación de usuarios, se pudo acceder ilegítimamente a datos personales de salud de ciudadanos mediante la introducción de números de DNI o NIE válidos de otras personas. Se inició un expediente sancionador porque las medidas de acceso eran muy débiles y erróneas. El responsable alegó que no se habían tomado más y mejores medidas de acceso por el elevado número de tratamientos y la situación de emergencia. Se consideraron infringidos los artículos 5.1.f) y 32 RGPD y se impusieron al responsable público dos sanciones de apercibimiento.

En este punto, el moderador, Pedro Alberto González, comentó que no existe demasiado control sobre los indicadores de sesión y se producen muchos casos similares, no necesariamente en el sector salud.

Otro caso fue el de una empresa privada que envió un mensaje de correo electrónico sin copia oculta, por lo que reveló las direcciones de correo electrónico al resto de pacientes. La investigación determinó que fue un error humano, pero al no haber medidas técnicas que minimizasen estos errores, se sancionó a la clínica.

Seguidamente, Juana Vegas Fernández expuso el caso de un paciente que acudió a un Centro de Salud con las consultas en obras y denunció que desde la sala de espera se escuchaban todas las conversaciones entre el médico y el paciente. Como solo había fotos, se realizó una inspección presencial en el Centro de Salud, constatando que era verdad que se escuchaban todas las conversaciones. Se sancionó al centro por no tomar las medidas adecuadas.

Al poco tiempo, llegó otra reclamación sobre los mismos hechos, se hizo una nueva inspección, pero en este caso no se escuchaba nada, ya que se habían realizado todas las medidas necesarias que se indicaron en la anterior reclamación, por tanto, en este caso, se desestimó.

Derecho de acceso

En primer lugar, Blanca Álvarez Yagüe expuso el caso de un particular que planteaba dudas sobre si el art. 15 del RGPD comprende conocer la identidad de los profesionales que acceden a la historia clínica. Hasta ahora ha sido que no, pero el Tribunal de Justicia Europeo no tiene la misma opinión, ya que indica que el derecho de acceso puede implicar hasta a la información subjetiva, siempre que sea sobre la persona en cuestión, por tanto, los datos personales que nos conciernen, también son los de terceros. Al mismo tiempo, indica que podría ser una vulneración de los datos de terceros. Por tanto, ya tenemos el conflicto creado. La solución es que no se podrá inadmitir directamente y no se tendrán que dar los datos de terceros, salvo fuera indispensable para el ejercicio del derecho. Esta sentencia solo se daría en caso de que hubiera un acceso indebido. Juana Vegas Fernández opinó que esta sentencia vendrá bien para poder ayudar más al paciente frente a los accesos indebidos.

A continuación, María Isabel Navarro Alonso expuso el caso de un reclamante que solicitó el acceso a su historia clínica, así como la información sobre los accesos a la misma, ya que sospechaba que su exmujer sabía que le iban a realizar una prueba médica. El responsable le facilitó los accesos, pero sin identificar a los profesionales, por tanto, puso una reclamación a la AEPD que solicitó al Servicio Cántabro de Salud la legitimidad de los accesos y este indicó que todos estaban relacionados con la relación profesional y asistencial del paciente y que no procedía la apertura de expediente a ningún profesional. Se archivó el caso, ya que el responsable contaba con un registro de acceso a la historia clínica, cumpliendo con el ENS y el reclamante no había constatado que se hubieran vulnerado esas medidas de seguridad.

Seguidamente, Juana Vegas Fernández expuso el caso de un reclamante que solicita los accesos a su historia clínica de su hijo, sin haber solicitado la tutela legal de forma oficial y haciendo la reclamación por teléfono. Esta reclamación fue inadmitida porque la solicitud no cumplía los requisitos básicos.

También expuso el caso de un reclamante que solicita el registro de accesos a su historia clínica en 2019 y lo vuelve a solicitar en 2023. El responsable denegó el derecho en 2023 alegando que era infundado o excesivo, al haber ejercido el derecho en 2019. La autoridad vasca consideró que no quedó demostrado su carácter infundado o excesivo y quien debía demostrarlo era el responsable. En este caso, había un procedimiento penal por medio por posibles accesos indebidos a la historia clínica.

Finalmente, María Isabel Navarro Alonso expuso el caso de un reclamante que vivía a más de 300 km de la clínica, por lo que había pedido el acceso a su historia clínica por correo o por correo postal. El responsable le respondió que tenía la información a su disposición, pero que debía recogerla presencialmente. El reclamante requirió que se la enviaran por correo electrónico cifrado. Según el responsable, como carecían de conocimientos informáticos, volvieron a insistir que debían entregarse de forma presencial. La AEPD estimó la reclamación por considerar que no se atendió debidamente el derecho de acceso.

También expuso el caso de una solicitud de acceso que realizaron las hijas menores de una señora que le hicieron una prueba mental y al no estar de acuerdo con los resultados solicitaron acceso a los test. El responsable manifestó que no podía dar una copia, por estar sujetas a derechos de autor y no contar con la autorización del mismo, pero les indicó que sí se las podían enseñar, ya que ya habían sido facilitados a la madre. Se estimó la reclamación por considerar que se debe ponderar el derecho de la parte reclamante a recibir una copia de los test solicitados y los derechos de autor. Por tanto, es posible atender el derecho mediante la modalidad de exhibición, pero siempre que se acredite que los test están sujetos a derechos de autor.

Otros derechos

En primer lugar, Nuria Pedros Ramos expuso el caso de una reclamación en representación de una hermana incapacitada por desatención de la solicitud del ejercicio del derecho de oposición. En su solicitud se oponía a que los datos personales que constan en la historia clínica compartida (HC3) de su tutelada fueran tratados por otros profesionales sanitarios o administrativos que no fueran una doctora determinada, indi-

cando que era ella la que tiene la potestad para decidir la información clínica que tiene que obrar a disposición de los distintos centros sanitarios que tratan a su hermana. La APDC desestimó esta reclamación por entender que se comprometía el derecho a la vida y la integridad física de la persona.

También expuso el caso de una reclamante que ejerció el derecho de supresión en relación con el diagnóstico "Depresión" de fecha 9 de agosto de 2019. En este caso, de conformidad con las alegaciones que presentó la entidad reclamada, la APDC resolvió desestimar el fondo de la reclamación, dado que no había transcurrido el plazo mínimo durante el cual dicho centro sanitario tiene que conservar esta información sobre la salud de la parte reclamante.

Finalmente, Juana Vegas Fernández expuso el caso de una solicitud de supresión de la totalidad de su historia clínica, porque entiende que al haber trasladado su domicilio a otra comunidad autónoma su historia clínica debe ser suprimida. El mero hecho de cambiar de domicilio a una comunidad autónoma diferente a la originaria no supone por sí solo el derecho a suprimir su historia clínica anterior, sino que deben cumplirse los requisitos exigidos en la ley para poder proceder a dicha supresión. Se estima formalmente la reclamación presentada contra el servicio vasco de salud al haber sido atendido el derecho de supresión ejercido por la reclamante extemporáneamente, pero se desestima la pretensión formulada por el reclamante, ya que los datos no pueden ser borrados al solo requerimiento del paciente, ya que existen normas específicas que obligan a conservar determinada información por plazos concretos y estas normas específicas prevalecen sobre el RGPD.

SÉPTIMA SESIÓN: SOLUCIONES DE SEGURIDAD ANTE EL TRATAMIENTO DE DATOS DE SALUD



El moderador, Miguel Ángel Benito Tovar, subdirector de Transformación, Innovación y Salud Digital del Servicio de Salud de las Illes Balears, destacó la importancia de la innovación en la seguridad de datos de salud.

En primer lugar, Ángel Villar Garea, Systems Engineer–SASE en Palo Alto, realizó la presentación "Cómo proteger tu dato esté donde esté" y destacó la importancia de la seguridad en todas las verticales, especialmente en el sector sanitario, donde recientemente se reportaron ataques de *ransomware*.

Los servicios ofrecidos por Palo Alto, incluyen la protección de redes, dispositivos y trabajo remoto. Se enfatiza la importancia del inventario de dispositivos y la detección de amenazas en el ámbito médico. Se discuten las soluciones para proteger el dato, incluyendo la prevención de la fuga de datos y el cifrado de documentos. Se muestra una demostración de cómo proteger los datos en dispositivos no gestionados. Finalmente, se resalta la capacidad de Palo Alto para proteger el dato en todas las aplicaciones corporativas.

A continuación, Javier Campo Azofra, sales engineer en Netskope, expuso la presentación "Cómo evitar fugas de información vía aplicaciones Generative IA y no fallar en el intento" y presentó una solución de ciberseguridad avanzada. Destacó la importancia de la transformación digital y cómo Netscope puede ayudar a proteger los datos y facilitar esta transición. Comparó la evolución en tecnología con ejemplos históricos como el cambio de carruajes a coches y la transformación de Netflix. Describió Netscope como una red de *data centers* distribuidos globalmente, certificados a nivel alto de seguridad. Explicó cómo Netscope garantiza la protección de datos, la inspección del tráfico y la detección de amenazas en tiempo real. Destacó la facilidad de escalabilidad y la capacidad de inspección profunda del tráfico sin impacto en el usuario. Igualmente, describió los servicios de ciberseguridad de Netscope, incluyendo acceso remoto basado en Zero Trust, Proxy, DLP y análisis de *malware*. Enfatizó en la educación del usuario en lugar de simplemente bloquear el acceso, y concluyó destacando la importancia de Netscope como una solución de seguridad en la nube para empresas y entidades gubernamentales en España.

Seguidamente, Alberto Martín de los Santos, director de Ciberseguridad en Inetum, realizó la presentación "Digitalizando la Salud: El 'Wallet Europeo' y la Revolución de la Identidad Soberana" y explicó la iniciativa del "*wallet* europeo" en el contexto de la digitalización de la salud y la identidad soberana. Destacó que el *wallet* europeo empodera al ciudadano al permitirle controlar cuándo, cómo y con quién comparte sus datos e identificación. También describió *cómo funciona el wallet* y mencionó que se espera que para el año 2030 el 80% de los ciudadanos europeos tengan acceso al mismo. Asimismo, expuso que el *wallet* centraliza la identificación del usuario y permite que este pueda compartir atributos específicos de forma segura y controlada. Además, mencionó que se está implementando un piloto de receta electrónica dentro del wallet en la Unión Europea, con el objetivo de facilitar la movilidad de los ciudadanos dentro de la UE y garantizar la autenticidad y seguridad de las recetas médicas. Este piloto busca evitar fraudes y garantizar que la entrega de medicamentos sea conforme a la prescripción médica original, independientemente del país de la UE en el que se encuentre el usuario. Además, explicó que el *wallet* funciona como una aplicación criptográfica que garantiza la seguridad de los datos personales y médicos del usuario.

Acto seguido, Axel Pérez García, sales engineer Iberia en Armis, expuso la presentación "Armis Centrix™ para la seguridad de los dispositivos médicos" y resaltó la importancia de mejorar la seguridad de los dispositivos médicos en entornos sanitarios. Señaló el aumento de dispositivos conectados en redes médicas y los desafíos para protegerlos, especialmente aquellos con sistemas operativos obsoletos. Describió la plataforma Armis como una solución basada en la nube que utiliza inteligencia artificial para descubrir, monitorear y proteger dispositivos conectados. Destacó la necesidad de colaboración entre diferentes departamentos para garantizar la seguridad de los dispositivos médicos. En conclusión, enfatizó la importancia de la visibilidad, comprensión del comportamiento y acciones proactivas para proteger los dispositivos médicos en entornos sanitarios.

Posteriormente, Darragh Kelly, socio y responsable de Alianzas Estratégicas Open Cloud Factory realizó la presentación "Seguridad Preventiva, Seguridad Dirigida" y compartió aprendizajes sobre ciberseguridad en el sector sanitario nacional. Destacó la necesidad de pasar de un modelo reactivo a uno preventivo en seguridad cibernética, especialmente centrado en identificar exposiciones ante amenazas como el *ransomware*. Explicó cómo su empresa, como fabricante de soluciones de ciberseguridad, se adapta a estas necesidades y se enfoca en colaboraciones estratégicas para abordar los desafíos específicos del sector sanitario. Resaltó la importancia de trabajar con socios especializados en el sector para ofrecer soluciones dirigidas y efectivas.

Para finalizar, Juan Miguel Auñón García, científico de datos en GMV, realizó la presentación "Seguridad en compartición de datos de salud" y habló sobre la seguridad en la compartición de datos de salud, centrándose en preservar la

privacidad de los pacientes para fines de investigación y el desarrollo de soluciones de inteligencia artificial. Propuso resolver este desafío mediante tecnologías de mejora de privacidad, como el aprendizaje federado. Presentó un caso de uso real sobre la predicción de lesiones de piel en un consorcio de investigación médica, destacando cómo la tecnología le permite compartir datos federados sin comprometer la privacidad y mejorar la generalización de los modelos de inteligencia artificial.

En el resumen de la sesión, destaca la importancia de preservar la identidad y la seguridad del dato en todas sus fases y se mencionan temas como la seguridad del dato en tránsito, la continuidad asistencial, la brecha digital, el empoderamiento ciudadano en el acceso a servicios y la eficiencia en la aplicación de medidas de seguridad.

SÉPTIMA SESIÓN: LÍMITES EN EL TRATAMIENTO MASIVO DE DATOS



El moderador, Joaquín Pérez Catalán, director de la División de Relaciones Internacionales de la Agencia Española de Protección de Datos, destacó la importancia del tratamiento masivo de datos en el avance de la Inteligencia Artificial y la historia de este enfoque. Se enfatizó en la necesidad de comprender y abordar los riesgos asociados con el tratamiento masivo de datos, incluidos aspectos temporales, volumen de datos y variedad de información. Se mencionaron las directrices del reglamento europeo de protección de datos y se resaltó que el tratamiento masivo puede aumentar el riesgo, por lo que es fundamental aplicar medidas de seguridad y salvaguardas apropiadas. A continuación, presentó e invitó a los ponentes a compartir sus perspectivas sobre los problemas y limitaciones en el tratamiento masivo de datos de salud.

En primer lugar, Juan Díaz García, coordinador del Comité Técnico de Seguridad y Protección de Datos de la SEIS, destacó los desafíos y limitaciones en el tratamiento masivo de datos de salud. Se discutió el papel de los comités de ética en la investigación y la necesidad de estandarizar los procesos en un entorno donde la digitalización ha sido anárquica. Mencionó la importancia de la seudonimización y la anonimización de datos, así como los desafíos en la evaluación de proyectos de investigación, como la identificación de muestras adecuadas y la separación funcional de datos. También abordó la confusión entre conceptos como datos anonimizados y seudonimizados y resaltó la necesidad de claridad en los procedimientos de evaluación de riesgos. Finalmente, se discutieron temas legales pendientes, como la definición de datos personales y se señaló la importancia de las evaluaciones de impacto y la espera de resoluciones judiciales relevantes.

A continuación, Jose Mario Cepeda Muñoz, responsable de la Oficina de Seguridad TI del Servicio de Salud de Castilla-La Mancha, abordó los desafíos de la gobernanza de datos masivos en el ámbito de la salud. Destacó la falta de formación especializada en la gestión y anonimización de datos, especialmente en el contexto de la inteligencia artificial. Además, mencionó la complejidad añadida por la normativa vigente sobre protección de datos y seguridad de la información, que requiere un análisis de riesgos exhaus-

tivo. En respuesta a estos desafíos, el Servicio de Salud de Castilla la Mancha ha creado una Dirección General de Salud Digital, que se enfoca en tres áreas proactivas: política de privacidad, ciberseguridad y transparencia de algoritmos. Se destacó la importancia de la implicación de la dirección y la necesidad de establecer un marco organizativo y normativo claro para abordar estos desafíos de gobernanza de datos.

Finalmente, **Ricard Martínez Martínez,** director de la Cátedra de Privacidad y Transformación Digital Microsoft de la Universidad de Valencia, abordó los problemas y riesgos en proyectos europeos de manejo masivo de datos, cuestionando la noción de límites en la protección de datos y resaltando la necesidad de condiciones de gobernanza.

Destacó las barreras políticas, culturales, materiales y jurídicas asociadas con la palabra "límite" en el contexto de la protección de datos. Además, señaló desafíos legales, como la diversidad de normativas nacionales y la necesidad de consentimiento específico para proyectos masivos de datos. También discutió restricciones de infraestructura y capacidades técnicas para la federación de datos, así como desafíos en la anonimización de datos. Presentó el enfoque de su equipo en desidentificación, eliminación de metadatos y compromisos jurídicos para garantizar la privacidad de los datos.

A continuación, el moderador, **Joaquín Pérez Catalán,** junto con el resto de ponentes, concretaron soluciones para abordar los problemas planteados anteriormente:

- Destacan la importancia de la formación y capacitación en protección de datos y el establecimiento de equipos multidisciplinares.
- Señalan la necesidad de políticas públicas que regulen el acceso y tratamiento de datos, así como la importancia de contar con personal cualificado en las organizaciones.
- Enfatizan la trazabilidad del proceso y la validación práctica de los datos.
- Abogan por políticas públicas integradas y un modelo de gobernanza efectivo.
- Por último, advierten sobre la importancia de revisar y mejorar las metodologías de análisis de riesgos en Inteligencia Artificial.

Para finalizar la sesión, se abrió la oportunidad de preguntar al público:

- Se planteó la preocupación sobre si la administración pública está preparada para contratar perfiles requeridos por normativas recientes, como delegados de protección de datos y analistas.
- Se discutió la necesidad de definir competencias y capacidades más allá de las titulaciones universitarias.
- Se mencionó la importancia de transmitir la necesidad de actuar ante los problemas identificados, pero se reconoce la dificultad para resolverlos debido a estructuras y decisiones administrativas.
- Se concluyó con la idea de seguir trabajando en lo que se puede, aunque el cambio pueda ser lento.

ACTO DE CLAUSURA

La clausura fue presidida por **Isabel López San Román,** directora asistencial del Hospital General Universitario de Toledo, en representación de **Alberto Jara Sánchez,** director-gerente del Servicio de Salud de Castilla La Manch. Intervinieron **Noemí Cívicos Villa,** directora general de Salud Digital y Sistemas de Información en el Sistema Nacional de Salud del Ministerio de Sanidad, y **Miguel Ángel Benito Tovar,** coordinador general del Foro de Seguridad y Protección de Datos de Salud.

En primer lugar, tomó la palabra **Miguel Ángel Benito**, quien empezó su participación agradeciendo a todos los participantes, organizadores, ponentes y colaboradores y destacando la importancia del Foro como punto de colaboración para afrontar las amenazas de ciberseguridad a la que se enfrenta el sector salud, tras lo cual a modo de resumen de las distintas mesas destacó las siguientes conclusiones:

- Se ha trabajado en la gestión de identidades en los Servicios de Salud, canales de comunicación con el ciudadano, la guía de gobernanza del dato, la seguridad de dispositivos médicos y la ocultación de la historia clínica.



- Se debe reaccionar ante la revolución de las tecnologías emergentes, tanto en la investigación, como en la asistencia sanitaria.
- Se debe afrontar el reto del gobierno de los nuevos espacios de datos, que trae consigo nuevos riesgos.
- La privacidad y la salud no se valoran hasta cuando se pierden, como indica Mar España en todos los foros.
- La importancia de la privacidad por diseño y por defecto desde el inicio de cualquier proyecto, tanto en el uso primario como secundario de los datos, para lo que es imprescindible el empoderamiento del paciente, para que sepa qué datos y qué uso se le dan.
- La importancia de la anonimización o preservación de la identidad del paciente como piedra angular en el uso secundario de los datos, para no permitir la reidentificación.
- La importancia del rol de los delegados de Protección de Datos para el diseño de los Espacios de Datos. Más del 30% de las brechas de seguridad se han producido en el sector sanitario.
- La Inteligencia Artificial generativa supone nuevos riesgos, que deberían afrontar con medidas preventivas, antes que reactivas.
- Los nuevos vectores de ataque, como dispositivos móviles y equipos IoT, generan que se deben aplicar nuevas medidas para evitar los ataques al sector sanitario.
- Destacan las guías de cumplimiento del ENS.
- Por último, destacaron el gran trabajo realizado dentro del proyecto CiberAP, con las reuniones en las que participan todas las CC AA, patrocinado y promovido por Noemí Cívicos Villa.

En segundo lugar, tomó la palabra **Noemí Cívicos Villa,** que mostró su agradecimiento a asistentes, proveedores, ponentes, autoridades y miembros del Comité, para posteriormente destacar las conclusiones derivadas del Foro:

- El lema del Foro refleja claramente la preocupación del sector sanitario. Desde el Ministerio se están invirtiendo recursos económicos en crecimiento desde 2017. La información de salud es muy valiosa.
- El sector sanitario necesita un marco estratégico, coordinado y compartido de protección de alertas específico del sector.
- Agradeció a las autoridades de Protección de Datos la exposición de casos prácticos que nos ayudan a mejorar en el día a día y a su asesoramiento experto es fundamental en nuestro sector.
- El uso secundario de datos es fundamental que se coordine en todos los ámbitos, sobre todo en el uso de Inteligencia Artificial, que ya tiene un borrador para regularse.
- El nuevo reto será la implantación del Sistema de Información para la integración de la información genómica a nivel nacional.

Para finalizar, tomó la palabra **Isabel López San Román,** que destacó la necesidad de liderar una transformación en la atención sanitaria, reconociendo la falta de preparación en el manejo de la protección de datos y la tecnología. Resaltó la importancia de entender y colaborar con actores externos, como la industria farmacéutica y tecnológica y expresó la urgencia de superar obstáculos y trabajar en conjunto para avanzar hacia una atención sanitaria pública eficaz. Para finalizar, agradeció la participación y dio por clausurado el evento.

FORO DE
INTEROPERABILIDAD

Coordina: **Adolfo Muñoz Carrero**

Introducción a openEHR

Como se comentó en la anterior entrega, el Programa de Especificaciones es uno de los 4 que tiene openEHR y es el encargado de desarrollar, gestionar y mantener las especificaciones y sus expresiones computables.

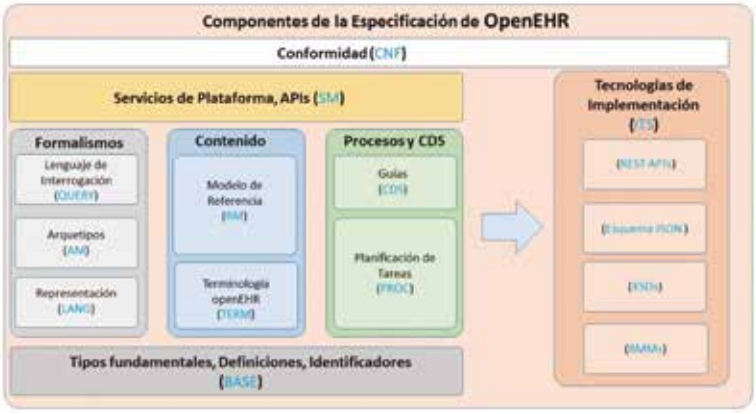
La figura muestra los componentes de la especificación de openEHR, que son la base de toda su formalización. La parte izquierda de la figura contiene las especificaciones (abstractas) independientes de la plataforma mientras que, a la derecha, tenemos las expresiones de dichas especificaciones en diferentes formalismos de implementación (REST, JSON, etc.) constituyendo las tecnologías de implementación (o ITS), que podremos usar en nuestros desarrollos. Cuando las tecnologías de implementación evolucionen en el tiempo, las ITS cambiarán y se adaptarán, pero las especificaciones abstractas (izquierda de la figura) se mantendrán, proporcionando estabilidad a la especificación openEHR.

Las especificaciones abstractas se organizan de la siguiente manera:

BASE: son las especificaciones de las definiciones, de los identificadores y de los tipos de datos fundamentales, que constituyen los tipos de datos primitivos que cualquier sistema debe implementar internamente y que openEHR asume (octeto, carácter, booleano, entero, entero64, real, doble y cadena).

FORMALISMOS: incluyen formalismos genéricos, dividido en 3 partes:

- **AM:** donde se describe el modelo de arquetipos (AM) y el lenguaje de descripción de arquetipos (ADL)
- **LANG:** se formalizan lenguajes genéricos para el resto de las especificaciones: ODIN, lenguaje de notación para instancias de objetos; BEL, lenguaje de expresiones básico; BMM, metamodelo básico de modelos y expresiones; EL, lenguaje de expresiones avanzado basado en BMM.
- **QUERY:** lenguajes de interrogación que formaliza el AQL, el lenguaje de interrogación basado en arquetipos.



CONTENIDO: donde se especifica el modelo de referencia (RM) en el que se basa la representación de los datos de openEHR y la terminología propia que usa openEHR para el resto de especificaciones.

PROCESOS y CDS: donde se definen los componentes referidos al proceso clínico y al soporte a la decisión clínica: GDL (lenguaje de definición de guías), TP (planificador de tareas, un flujo de trabajo clínico adaptativo, ejecutable y basado en equipos), TP_VML (lenguaje visual de modelado para planes clínicos y flujos de trabajo)

CONFORMIDAD: estas especificaciones definen los criterios de conformidad, incluye la definición formal de la plataforma openEHR y cómo testarla. Incluye también los mecanismos para certificar productos openEHR y para crear requisitos para procesos de compra.

Se pueden consultar todas las especificaciones en el siguiente enlace: https://specifications.openehr.org/development_baseline

SEGURIDAD Y PROTECCIÓN DE DATOS

Coordina: **Juan Díaz**

Designación y situación de los delegados de protección de datos

La Agencia Española de Protección de Datos (AEPD) ha participado en una acción europea coordinada para analizar la designación y situación de los delegados de protección de datos (DPD) en entidades públicas y privadas, dentro del marco de actuaciones coordinadas del Comité Europeo de Protección de Datos (EDPB, por sus siglas en inglés). Este documento proporciona una visión integral para identificar y fomentar las mejores prácticas, detectar posibles deficiencias y realizar recomendaciones. La figura del delegado de protección de datos ejerce una función fundamental de intermediación entre las Autoridades de Supervisión, la ciudadanía y las organizaciones, y contribuye de manera esencial al cumplimiento de la normativa de protección de datos y a promover la protección efectiva de los derechos de los interesados.

El informe, que ofrece una visión europea tanto del sector público como del privado, aglutina los resultados de las 25 autoridades de protección de datos que han participado en la iniciativa. Su finalidad es contribuir a elevar el nivel de cumplimiento y la protección de los datos personales de los ciudadanos, no sólo a nivel nacional sino también en el conjunto de la UE. Los resultados se muestran en el informe de forma agregada, generando una visión amplia y permitiendo un seguimiento específico en el ámbito del Espacio Económico Europeo.

Por su parte, la AEPD ha analizado las prácticas de las más de 10.000 entidades del sector público y privado que han respondido al cuestionario remitido y que incluía cuestiones relacionadas con la designación, conocimiento y experiencia de los DPD, sus tareas y recursos o su papel y posición en sus respectivas organizaciones, entre otras. En el caso de los cuestionarios dirigidos a las entidades del sector público andaluz, la Agencia ha colaborado con el Consejo de Transparencia y Protección de Datos de Andalucía, que ha publicado los resultados de dichas encuestas en su página web.

Por lo que respecta a entidades del sector privado, el cuestionario se ha dirigido a distintos sectores de actividad: educación, entidades bancarias y financieras, sanidad, sector energético, seguridad, servicios de telecomunicaciones, solvencia patrimonial y crédito, y actividades relacionadas con los juegos de azar y apuestas.

El informe recoge recomendaciones y puntos de atención dirigidos a las organizaciones, los DPD y las autoridades de control, tales como:

- Continuar promoviendo la concienciación entre las organizaciones para que adopten la necesaria diligencia en la designación del DPD.
- Necesidad de que los responsables del tratamiento verifiquen los medios puestos a disposición de los DPD para que desempeñen con eficacia las funciones que tienen encomendadas.
- Proporcionar la capacitación y la formación de los DPD a través de diversos mecanismos, así como fomentar el uso de la certificación.
- Necesidad de dotar al DPD de la debida independencia en el ejercicio de sus funciones con el fin de evitar los conflictos de interés, así como promover la necesaria visibilidad del delegado dentro de la organización.
- Importancia de promover los mecanismos internos para que el DPD reporte al más alto nivel de la organización.
- Continuar con la labor desarrollada hasta ahora por las autoridades de control con el fin de proporcionar directrices y herramientas que contribuyan al eficaz desempeño de las funciones de delegado de protección de datos.

FORO DE
SALUD CONECTADA

Coordina: **Oscar Moreno**

La imagen médica se hace móvil para mejorar la asistencia sanitaria (II)

Siguiendo en el ámbito de la imagen médica para mejorar la asistencia sanitaria, desarrollando dispositivos de ultrasonidos portátiles y empezado en el pasado número, veremos otra iniciativa financiada por la UE, llevada a cabo por investigadores de Bélgica y que tratan de generalizar la ecografía para un mayor número de usos sanitarios.

Este grupo de expertos está desarrollando una sonda de ultrasonidos portátil que debería facilitar los diagnósticos de los médicos y mejorar desde la asistencia a la maternidad hasta el tratamiento de lesiones deportivas.

El proyecto se llama LucidWave y tiene una duración de tres años, hasta mediados de 2025. Los aparatos portátiles que se están desarrollando miden unos 20 centímetros y tienen forma rectangular.

Los objetivos principales del proyecto incluyen el desarrollo y el suministro de dos prototipos funcionales y la evaluación de su rendimiento en el entorno clínico, además de proporcionar datos para su posterior validación clínica formal en el marco de las normativas relativas a productos sanitarios.

El equipo de LucidWave quiere que estén disponibles no sólo en los departamentos de radiología, sino también en otros lugares de los hospitales, como quirófanos o incluso residencias de ancianos.

Queremos ofrecer imágenes médicas por ultrasonidos portátiles e inalámbricas", explica Bart van Duffel, miembro del proyecto y director de innovación en tecnología de membranas, superficies y películas finas de la Universidad KU Leuven, en la región belga de Flandes.

Para ello, el equipo ha introducido en la sonda una tecnología de transductores diferente que utiliza sistemas microelectromecánicos, o MEMS, comparables a los chips de los teléfonos inteligentes.

La tecnología alternativa se basa en transductores ultrasónicos piezoeléctricos micromecanizados, o PMUT, diminutos "tambores" de película de silicona que vibran cuando se exponen a un voltaje y producen las ondas ultrasónicas necesarias para obtener imágenes que pueden abarcar diversas partes del cuerpo humano.

Las imágenes generadas son analizadas por el software LucidWave, que incluye inteligencia artificial y puede procesar rápidamente los datos y ofrecer un prediagnóstico a los expertos médicos.

El prototipo del proyecto es fácil de usar, por lo que pueden utilizarlo todo tipo de profesionales médicos y sanitarios, no sólo ecografistas", explica Sina Sadeghpour, directora de investigación de la Universidad Católica de Lovaina y responsable de LucidWave.

El equipo está probando el prototipo en cadáveres con el objetivo de mejorar la calidad de la imagen, un paso importante para solicitar permiso para realizar ensayos con personas vivas y, en última instancia, comercializar el dispositivo.

Los investigadores calculan que el dispositivo podría estar totalmente aprobado y comercializado en unos cinco años.

Queremos que las imágenes por ultrasonidos sean accesibles y asequibles sin comprometer su funcionalidad y rendimiento", afirma van Duffel. Vemos esta nueva tecnología de ultrasonidos como una especie de estetoscopio del futuro".

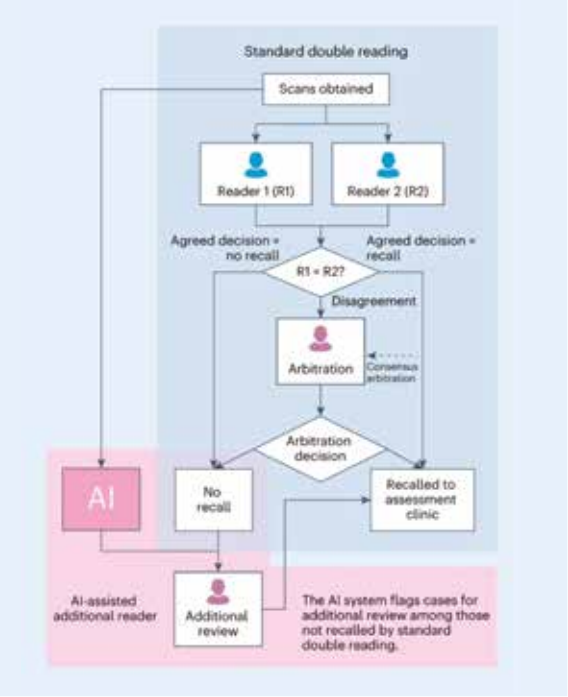
Más información:

- Comisión Europea - Horizon Magazine - https://projects.research-and-innovation.ec.europa.eu/en/horizon-magazine
- Proyecto LucidWave - https://cordis.europa.eu/project/id/101057902

INFORMÁTICA **MÉDICA**

Coordina: **Gregorio Gómez**

El uso de la IA puede mejorar la efectividad y la eficiencia de los programas de cribado de cáncer de mama, aunque podría implicar un mayor uso de recursos humanos



La transición hacia la atención médica impulsada por la IA es inevitable, pero debe realizarse con precaución y poniendo el foco en la seguridad y la eficacia. Este es el planeamiento en el que incide un reciente editorial de *Nature medicine*[1]. En él reivindica la necesidad de estudios clínicos cuidadosamente diseñados y de una implementación de algoritmos y dispositivos de IA en el mundo real que esté basada en la evidencia científica.

Un ejemplo de este enfoque es el que se encuentra en otro artículo publicado el 16 de noviembre de 2023 en la misma revista y en el que se evalúa el efecto de incorporar una lectura adicional mediante IA a la doble lectura habitual en los programas de cribado de cáncer de mama.

El estudio consistió en una evaluación prospectiva en tres fases:

- Fase 1 con el pilotaje en un solo centro y en la que se procesaron 3.817 mamografías con lectura doble estándar y 3.746 mamografías con lectura adicional asistida por IA.
- Fase 2 con un piloto multicéntrico en 4 centros y en la que se procesaron 9.266 mamografías con lectura doble estándar y 9.112 mamografías con lectura adicional asistida por IA.
- Fase 3 despliegue completo en la práctica real de 4 centros y en la que se procesaron 16.256 mamografías con lectura doble estándar y 15.953 mamografías con lectura adicional asistida por IA.

La incorporación de la lectura adicional mediante IA es la que viene esquematizada en la figura. El sistema de IA realiza una revisión adicional en los casos clasificados por doble lectura como negativos. Si alguno de ellos la IA lo identifica como positivo, discrepando con los lectores humanos, entonces se revisa adicionalmente por un árbitro humano para decidir si hay que citar a la paciente. En ese caso, la IA proporciona al árbitro adicional imágenes con regiones de interés destacando las áreas sugestivas de malignidad.

El resultado indica que, comparado con la lectura doble, la implementación de la lectura adicional asistida por IA logró detectar 0,7-1,6 casos adicionales de cáncer por cada 1.000 casos, con un incremento del valor predictivo positivo del 0.1-1.9%. La mayoría de los casos de cáncer detectados por la lectura asistida por IA fueron invasivos (83.3%) y de tamaño pequeño (⩽10 mm, 47.0%). Este estudio proporciona evidencia de que, si bien la lectura asistida por IA requiere lecturas adicionales, su mayor valor predictivo positivo sugiere que aumenta la efectividad del cribado y la eficiencia del proceso. También proporciona un ejemplo de uso de la IA en el que ésta no implica una reducción de los profesionales que participan en el proceso de cribado, sino que, por el contrario, aumenta ligeramente su necesidad, al incorporar la revisión asociada al arbitraje adicional.

1 How to support the transition to AI-powered healthcare. Nat Med 30, 609–610 (2024). https://doi.org/10.1038/s41591-024-02897-9
2. Ng, A.Y., Oberije, C.J.G., Ambrózay, É. et al. Prospective implementation of AI-assisted screen reading to improve early detection of breast cancer. Nat Med 29, 3044–3049 (2023). https://doi.org/10.1038/s41591-023-02625-9

SECTOR
ENFERMERÍA

Prueba de concepto basada en el uso de la inteligencia artificial para la optimización del modelo de predicción de fecha de parto

Ainara Alútiz Cañedo. Matrona. Subdirección de Enfermería, Dirección General. Osakidetza

La inteligencia artificial (IA) está adquiriendo gran relevancia como herramienta de apoyo en el ámbito de los cuidados y la salud. Su versatilidad y las amplias aplicaciones que ofrece convierten a la IA en un recurso que permite el avance y la mejora en la atención sanitaria

Durante muchos años, la predicción de la fecha de parto ha sido foco de interés en el campo de la obstetricia, teniendo como fin último el de mejorar los resultados de salud tanto para las gestantes como para los recién nacidos. La precisión en la predicción de la fecha de parto es crucial, especialmente en los casos de riesgo de parto pretérmino o postérmino, ya que contribuye a optimizar los cuidados en la atención perinatal, disminuye la ansiedad materna y aumenta la eficiencia en la gestión de recursos. Es en este escenario donde la IA se postula como un instrumento de gran utilidad.

Con el fin de comprobar la viabilidad de la optimización del modelo de predicción de la fecha de parto a través del uso de técnicas de aprendizaje automático (Machine Learning), un equipo multidisciplinar de Osakidetza-Servicio Vasco de Salud llevó a cabo una prueba de concepto a lo largo del segundo trimestre de 2022. Utilizando algoritmos de árboles de decisión, redes neuronales y modelos de regresión, se trató de comprobar la precisión de las estimaciones de la IA comparándola con la de los modelos tradicionalmente utilizados.

Se analizaron de forma retrospectiva las variables con datos estructurados asociados a gestación de mujeres cuyo embarazo y parto fueron atendidos en Osakidetza entre 2019 y 2022. Tras entrenar los algoritmos, se realizaron cinco modelos para estimar los días de gestación que restaban hasta el parto y cuatro modelos de clasificación binaria para parto prematuro o postérmino en distintos cortes temporales a lo largo del embarazo.

Los modelos generados revelaron una sobreestimación en la predicción de la fecha de parto, sin embargo, se observó un nivel de acierto del 23.55% al 25.51% sobre la fecha real del parto y los cinco días posteriores. Aunque estos resultados no superaron significativamente a los modelos tradicionales, la prueba de concepto arrojó conclusiones valiosas que sirven como punto de partida de mejoras y avances en esta línea.

Por un lado, una limitación destacada fue la imposibilidad de utilizar datos no estructurados, dado lo complejo de su extracción, a pesar de contener gran volumen de información relacionada con el embarazo. Actualmente, las organizaciones están trabajando para avanzar en la gestión adecuada y el gobierno de los datos, esfuerzo que repercutirá positivamente en este tipo de proyectos.

Por otro lado, como se ha mencionado, el estudio desarrolló en un tiempo limitado nueve modelos con tres variables objetivo distintas, lo que impidió la evolución individual de cada uno de ellos, dejando abierta una vía de desarrollo para futuras investigaciones.

En resumen, la integración de la IA en el ámbito de la salud promete avances significativos en la atención perinatal. Aunque la prueba de concepto reveló desafíos y limitaciones, también proporcionó insights valiosos que impulsarán futuras investigaciones y mejoras en la gestión de datos y en el desarrollo de modelos más precisos y eficaces.

SECTOR
FARMACIA

Coordina: **Comité Tecnológico de Farmacia de la SEIS**

Características de la receta electrónica en Estonia

Anett Lilleväli. Analista de Tecnologías de la Información. Fondo de Seguro Médico de Estonia.
Patrick Pihelgas. Director de proyecto. Fondo de Seguro Médico de Estonia.
Rutt Lindström. Responsable de Análisis de Datos. Centro de Sistema de Información para el Bienestar y la Salud.
Luz Fidalgo García. Coordinadora del Comité Tecnológico Farmacéutico de la SEIS.

¿Podría describir su sistema de eprescripción/edispensación? ¿Cuánto tiempo lleva funcionando?

El sistema de receta electrónica de Estonia fue lanzado en 2010 por el Fondo de Seguro Médico de Estonia. Un año después de su lanzamiento, el 84% de las recetas se emitían de forma digital. Hoy en día, la receta electrónica es un sistema nacional, centralizado y sin papel utilizado por todos los médicos, pacientes y farmacias. En 2024, el 99,95% de las recetas son ya electrónicas y se emiten alrededor de 14 millones de recetas cada año, lo que se traduce en un importante ahorro de tiempo para todas las partes.
La base de datos central es "Prescription Center", que ofrece diferentes servicios para los médicos, los farmacéuticos y los pacientes, lo que implica una integración con varios registros estatales. La base de datos central es la columna vertebral del servicio, ya que recopila y verifica datos relevantes de diferentes registros:

- Identificación del derecho a prescribir o dispensar medicamentos.- Registro de licencias de prestación de Servicios de Salud, Registro de Profesionales de la Salud y Registro Nacional de Farmacéuticos. Estos registros son gestionados por la Junta de Salud.
- Identificación de las sustancias farmacéuticas, la licencia de comercialización, las dosis estándar.- El Registro de Medicamentos, gestionado por la Agencia Estatal de Medicamentos. También gestiona el registro de licencias de actividad de las farmacias.

Todos los proveedores de servicios de atención médica y las farmacias están conectados al sistema central de recetas electrónicas y, después de recetar un medicamento, el sistema central almacena la receta entrante, pudiendo tener acceso a ella inmediatamente desde el sistema de información de cada farmacia, previa solicitud.

Desde su punto de vista, ¿qué característica es la más relevante en su sistema electrónico?

La característica más importante de nuestro sistema es probablemente la amplia adopción y aceptación por parte de nuestros usuarios. Hoy en día, el 99,95 % de las recetas emitidas en Estonia son electrónicas, lo que significa que tenemos toda una generación de jóvenes que ni siquiera han visto una receta en papel.

¿Qué mejoraría en el sistema y en qué líneas de mejora se está trabajando ahora?

Actualmente, estamos trabajando en un nuevo servicio llamado Esquema de Medicamentos. Esta es una solución que creemos debería convertirse en la nueva práctica estándar de prescripción de medicamentos.
El plan de medicación es la lista de tratamientos de un paciente: para los médicos, la atención se centraría exclusivamente en los tratamientos y las recetas funcionarían más como elementos logísticos en segundo plano. Por ejemplo, un tratamiento de por vida aparecería en el esquema de medicación como una fila continua, no como una enorme colección de recetas bimestrales.

Esto permite una mejor planificación de nuevos tratamientos, así como una visión general más clara de los tratamientos anteriores. Y hará más fácil detectar posibles interacciones o sospechas de efectos secundarios, y los médicos asumirán la responsabilidad de cambiar todo el esquema de medicación en lugar de simplemente añadir una receta. Y, por supuesto, los pacientes también tendrían una visión mucho mejor de su lista de medicamentos actual.
El sistema de prescripción actual incluye únicamente recetas dispensables en oficinas de farmacia. El Esquema de Medicamentos permitirá agregar medicamentos de venta libre que informe el paciente, lo que supondrá una mejora para la detección de interacciones con medicamentos de venta libre.
Un avance futuro muy importante es la digitalización, en un sistema central, de los medicamentos para pacientes hospitalizados.
Otro desarrollo futuro interesante es un apoyo a la toma de decisiones, que tendría en cuenta los datos genéticos personales del paciente en el momento de la prescripción de medicamentos como parte de la atención médica habitual. El Instituto Nacional para el Desarrollo de la Salud ha finalizado el proyecto "Implementación de la medicina personalizada en Estonia", durante el cual la infraestructura informática de la medicina personalizada permite el uso de datos genéticos al prescribir medicamentos. En los próximos años, al prescribir medicamentos, los médicos deberían poder acceder al sistema de alerta de interacción gen-fármaco específico del paciente en su propio sistema de información.

En relación al pago del paciente en farmacia, ¿el paciente paga la cantidad total o sólo un porcentaje del precio de cada producto? ¿Cómo se hace eso en su sistema eP/eD?

En Estonia, la prescripción basada en DCI es obligatoria y hemos establecido los precios de referencia que estamos dispuestos a pagar por los medicamentos cubiertos por el Fondo de Seguro Médico de Estonia.
El precio de referencia es el segundo precio más bajo del mercado y se establecen y actualizan trimestralmente. Hay cuatro tipos de reembolso:100%, 90%, 75% y 50% y el descuento se calcula sobre el importe restante del precio de referencia, que es el precio de referencia menos 2,5 €. Estos 2,5 € son un copago fijo del paciente. Si el precio del medicamento es superior al precio de reembolso, el paciente deberá pagar el resto además de cualquier copago.
El sistema de receta electrónica también está integrado con la base de datos de seguros, donde recopilamos datos sobre el ciudadano, el tipo de seguro, el proveedor de seguro (quién paga el impuesto social por esta persona), por lo que con esta información podemos identificar el derecho a ser reembolsado. Para medicamentos, el sistema de receta electrónica también permite el cálculo automático de la tasa correcta de reembolso de los medicamentos cubiertos por la Caja del Seguro Médico.

Desde hace un tiempo, puedes intercambiar recetas con otros países europeos. ¿Podrías decirnos con qué países y cuánto tiempo lleva funcionando con cada uno?

El primer servicio transfronterizo de recetas electrónicas se lanzó en 2020/2021 con Finlandia. Ahora mismo podemos intercambiar recetas y dispensaciones transfronterizas con siete países (entre ellos España). Durante estos años, hemos observado que la demografía de los usuarios del servicio es diferente entre países: por ejemplo, la receta electrónica estonia en Finlandia es utilizada mucho por los estonios que trabajan en Finlandia, mientras que la receta electrónica finlandesa en Estonia es más utilizada por turistas.
Lo que dificulta la receta electrónica transfronteriza son las diferencias en los sistemas nacionales de prescripción y registros de medicamentos, y los flujos de trabajo nacionales a los que están vinculados. Un servicio de prescripción que esté plenamente operativo a nivel nacional puede plantear desafíos inesperados cuando se "traduce" al sistema de dispensación de otro país. Incluso cuando abordamos con éxito las cuestiones relacionadas con el mapeo y la traducción de los datos, a menudo es la lógica empresarial la que hace que las recetas no sean dispensables o no sustituibles en otro país.

Encuentre más información sobre el intercambio de datos transfronterizo en el sitio web de TEHIK (https://www.tehik.ee/).

XIV REUNIÓN • 29 Y 30 DE MAYO • 2024

Foro para la Gobernanza de las TIC en Salud

El Foro de Gobernanza de las TIC en Salud tiene por objetivo contribuir al desarrollo profesional especializado en informática de la salud en las instituciones, mediante la participación de todos los agentes involucrados en la toma de decisiones, y en concreto, promover un entorno colaborativo de comunicación del conocimiento e intercambio de información científico-técnica entre los profesionales y directivos en informática de la salud. Por ello, el lema elegido para esta edición es: "El modelo colaborativo en el desarrollo de la Estrategia de Salud Digital". Las mesas de debate que tendremos en la reunión de este año son: Plan de Atención Digital Personalizada y Red ÚNICAS y el Plan de un Sistema de Información Nacional de Genética durante el primer día, y en el segundo: Plan de Transformación Digital de Atención Primaria, IA Generativa en el sector sanitario y Liderazgo y claves para la Gestión del Cambio.

En las tres primeras mesas de los planes se detallará su evolución y situación actual y en las dos últimas se abordará por un lado la tecnología IA Generativa que está suscitando el interés de todas las organizaciones sanitarias por su implicación, y por otro un aspecto de gestión fundamental como es la gestión del cambio.

Contaremos con participación de referentes del sistema nacional de salud, así como de la sanidad privada y de la industria, y nos darán su opinión sobre todos estos temas que están en la agenda de la Estrategia de Salud Digital.

PROGRAMA

29 DE MAYO DE 2024

16.00 - 16.30 Registro de Participantes

16.30 - 17.00 Acto de Apertura

17.00 - 18.30 Sesión Debate 1

"Plan de Atención Digital Personalizada y Red ÚNICAS"

Se hablará del estado actual del proyecto UNICAS (red para la atención de pacientes con enfermedades raras) tras un año de su inicio. Se pondrán en común tanto los avances registrados en este tiempo como las dificultades, enseñanzas y previsiones futuras.

18.30 - 18.45 Descanso

18.45 - 20.15 Sesión Debate 2

"Plan SiGenEs (S.I.Genetica nacional)"

CCAA. En esta sesión se detallará los objetivos del plan que incluyen la ampliación del catálogo de pruebas genómicas en el SNS y el desarrollo de un sistema de información para la integración de información a nivel nacional.

21.30 Cena coctail - Restaurante Bellavista

30 DE MAYO DE 2024

09.30 - 11.00 Sesión Debate 3

"Plan de Transformación Digital de Atención Primaria"

Desarrollo de las distintas líneas de trabajo y los proyectos colaborativos seleccionados y puestos en marcha, con la participación de CCAA que han actuado como líderes y empresas con experiencias nacionales e internacionales en este ámbito.

11.00 - 11.30 Pausa Café

11.30 - 12.45 Sesión Debate 4

"IA Generativa en el sector sanitario"

Distintos ámbitos de actuación de esta tecnología en la salud, beneficios y posibles riesgos. Iniciativas existentes en la actualidad y papel que están desarrollando los distintos agentes implicados en su desarrollo.

12.45 - 14.00 Sesión Debate 5

"Liderazgo y claves para la Gestión del Cambio"

La eficiencia de los proyectos TIC destinados a la transformación digital de Salud está fundamentada en la gestión del cambio. Se trata de un área trasversal sobre la que Europa está poniendo el foco de atención. Experiencias y modelos de gestión del cambio

4.00 - 14.30 Acto de Clausura

AGENDA 2024

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

XIV REUNIÓN DEL FORO DE INTEROPERABILIDAD Y GOBERNANZA DEL DATO EN SALUD

Fecha: 24 y 25 abril · **Lugar:** Zaragoza

XIV FORO PARA LA GOBERNANZA DE LAS TIC EN SALUD

Fecha: 29 y 30 mayo · **Lugar:** Gijón

XXXI JORNADAS NACIONALES DE INNOVACIÓN Y SALUD EN ANDALUCÍA

Fecha: 23, 24 y 25 de octubre · **Lugar:** Málaga-Torremolinos

XXII REUNIÓN DE SALUD CONECTADA

Fecha: 20 y 21 noviembre · **Lugar:** Navarra

X MÁSTER EN DIRECCIÓN DE SISTEMAS Y TICS PARA LA SALUD

Fecha: noviembre 2023 - octubre 2024

solventum

3M Health Care
es ahora Solventum

Lo que no cambia es nuestro compromiso para asegurar la calidad del dato clínico mediante soluciones integrales que hagan más fácil el trabajo de los codificadores con herramientas semiautomáticas que mejoren la eficiencia y precisión, sin olvidarnos de sistemas de ayuda a los clínicos para que documentar con calidad sea fácil y merezca la pena.

¡Confíe en nosotros para impulsar el futuro de la atención médica basada en evidencias!

Organiza

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

XIV Reunión

Foro para la Gobernanza de las TIC en Salud

"El Modelo Colaborativo en el Desarrollo de la Estrategia de Salud Digital"

GIJÓN

29 y 30 de mayo de 2024

ABBA PLAYA GIJÓN HOTEL
Paseo Doctor Fleming, 37
33203 Gijón

Síguenos en twitter:
@SEISeSalud

SOCIO TECNOLÓGICO PRINCIPAL

Abbott · Dedalus · dexcom · FUJITSU · Microsoft · minsait | sia An Indra company

SOCIO TECNOLÓGICO COLABORADOR

FUJIFILM Value from Innovation · PHILIPS · Roche · salesforce · T Systems · SIEMENS Healthineers