LOS RETOS QUE MARCA LA CIBERSEGURIDAD DEL DATO SANITARIO

La sanidad avanza hacia un modelo cada vez más digital, interconectado y dependiente del dato. Sin embargo, este progreso trae consigo un desafío crítico: proteger la información clínica en un entorno donde su volumen, valor y exposición no dejan de crecer.
La ciberseguridad ya no es sólo una cuestión técnica, sino un pilar estratégico para garantizar la continuidad asistencial, la confianza del paciente y la sostenibilidad del sistema sanitario.

Salvador Luna
Digital Marketing & Corporate Communications Manager en Fujifilm España

La digitalización sanitaria ha transformado el diagnóstico, tratamiento y acompañamiento de los pacientes. Y, junto a ella, ha emergido un reto que ya no puede considerarse exclusivamente tecnológico: la ciberseguridad del dato clínico. Proteger la información sanitaria es una obligación legal y una condición imprescindible para garantizar la continuidad asistencial y la confianza del paciente.

En España y en el conjunto de la Unión Europea, el marco normativo es exigente: el Reglamento General de Protección de Datos (RGPD) establece que la información relativa a la salud es una categoría especialmente sensible y requiere el máximo nivel de protección.

A nivel nacional, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales refuerza estas obligaciones, mientras que la Ley 41/2002 regula la autonomía del paciente y la documentación clínica, estableciendo que las historias clínicas deben conservarse, como mínimo, durante cinco años desde la fecha de alta de cada proceso asistencial.

Además, en la práctica, muchas comunidades autónomas y centros sanitarios amplían significativamente estos plazos, especialmente en el ámbito del diagnóstico por imagen, donde la trazabilidad a largo plazo resulta esencial.

Y es aquí donde surge una de las grandes paradojas del sistema: cada vez generamos más datos,

que hay que guardar durante más tiempo y con mayor nivel de detalle, lo que amplía también la superficie de riesgo.

Una resonancia magnética de alta resolución, un estudio de tomografía computarizada multicorte o una digitalización completa en anatomía patológica no son archivos ligeros. Son conjuntos de datos de enormes dimensiones que deben almacenarse durante años —a veces décadas— y estar disponibles cuando el profesional los necesite.

> La imagen médica moderna ya no es una placa aislada; es un ecosistema de información interconectada.

Los sistemas PACS, las plataformas de visualización 3D, los entornos de inteligencia artificial y las soluciones de interoperabilidad multiplican el valor clínico del dato, pero también su exposición.

Cada punto de conexión, cada integración con terceros, cada acceso remoto representa una potencial vulnerabilidad si no se gestiona adecuadamente.

> Es más, hemos visto que los ciberataques a hospitales se han convertido en una amenaza real. Y que cuando un centro sanitario sufre un incidente de seguridad, no sólo se comprometen datos: también la actividad quirúrgica, la programación de pruebas diagnósticas, la atención urgente...

Ante esta situación, la respuesta no puede limitarse a reforzar cortafuegos o a confiar exclusivamente en soluciones en la nube. Necesitamos una estrategia integral que combine prevención, segmentación, copias de seguridad robustas y planes de recuperación ante desastres. Y aquí adquiere especial relevancia el concepto de *air-gap*: mantener copias de seguridad físicamente desacopladas de la red principal para evitar que un ataque las comprometa.

En el ámbito del almacenamiento a largo plazo, esta aproximación cobra especial sentido. Existen soluciones "llave en mano" que permiten a los centros sanitarios gestionar grandes volúmenes de información —incluso superiores al *petabyte*— en sus propias instalaciones, con un modelo de archivo seguro y energéticamente eficiente. Este tipo de infraestructuras pueden desacoplarse de la red crítica, ofrecen una capa adicional de protección frente a ataques masivos de *ransomware* y contribuyen a garantizar la disponibilidad futura del dato clínico.

> No se trata de plantear un debate entre nube y almacenamiento local, sino de entender que la arquitectura debe ser híbrida y resiliente.

Los datos de uso frecuente pueden residir en entornos de acceso rápido, mientras que el archivo histórico —que por ley debe conservarse y que clínicamente puede ser necesario años después — puede protegerse en sistemas diseñados específicamente para la preservación segura y sostenible.

Por otra parte, la seguridad del dato no depende únicamente de la tecnología, sino también de los procesos y de las personas. Hay que invertir en formación continua, protocolos de acceso, autenticación multifactor, auditorías periódicas y evaluación de proveedores para conformar una gobernanza responsable del dato sanitario. La futura consolidación del Espacio Europeo de Datos de Salud reforzará aún más esta exigencia de control, trazabilidad y reutilización segura de la información.

La transformación digital de la sanidad sólo tendrá sentido si es segura.

Podemos incorporar inteligencia artificial, interoperabilidad avanzada y modelos híbridos de atención, pero todo ello descansa sobre un pilar fundamental: la integridad, la disponibilidad y la confidencialidad del dato. Sin esa base responsable y segura, toda innovación en la que invirtamos perderá su valor.