Ciberataques: el enemigo latente

Dilenny Camacho Diplán

Desde la publicación de mi último artículo, *Smart Hospital (hospitales inteligentes): retos de la transición,* ha surgido una serie de inquietudes y reflexiones en relación a ciertos retos latentes en cuanto a la transición de este tipo de hospitales y de la gestión que se debe hacer en los centros de salud. Uno de los tópicos que más comentaron fue el hecho de los ciberataques y de cómo estamos enfrentando este riesgo.

La digitalización de los servicios sanitarios ha traído grandes avances en eficiencia y capacidad de respuesta clínica. Sin embargo, también ha incrementado la superficie de exposición frente a amenazas cibernéticas cada vez más sofisticadas. El sector salud es hoy uno de los blancos principales de los ataques tipo *ransomware* (códigos maliciosos). En este sentido, la alta dirección de los hospitales enfrenta un doble desafío: comprender la naturaleza del riesgo y tomar decisiones estratégicas en un contexto de restricciones presupuestarias, y el déficit de talento especializado y tecnicismos que alejan a los equipos directivos del problema real.

Evidentemente sería un atrevimiento por mi parte abordar este tema sin ser especialista, pero quiero llamar a la reflexión desde el sillón de los gestores y de cómo vemos este proceso al que nos estamos enfrentando, siendo esto una amenaza creciente y que afecta de manera directa la misión asistencial a lo que estamos llamados.

De acuerdo con el informe *State of Ransomware in Healthcare 2024*, elaborado por Sophos (2024), el 67% de las organizaciones sanitarias sufrieron al menos un ataque de *ransomware* en el último año, lo que representa el mayor incremento en cuatro años. Esta cifra no solo refleja una mayor frecuencia de ataques, sino también su creciente sofisticación y capacidad de paralizar procesos clínicos críticos.

Ahora bien, uno de los mayores retos que tienen nuestros hospitales es la barrera interna de la dificultad que enfrentan los miembros del consejo de dirección para comprender y liderar la gestión del

riesgo cibernético. En muchos casos, las decisiones estratégicas se toman desde una comprensión limitada de los términos técnicos, lo que se traduce en planos de acción incompletos, presupuestos reactivos y subestimación del problema.

La experiencia del Hospital Clínico de Barcelona ilustra esta brecha. Tras el ciberataque que sufrió en marzo de 2023, que paralizó más de 11.000 consultas externas y 300 cirugías, la institución se vio obligada a revisar completamente su estructura de seguridad digital (*El País*, 2023). El rescate exigido por los atacantes ascendía a 4,5 millones de dólares, y más de 4,5 terabytes de información fueron robados.

Asimismo, el Hospital Universitario de Caldas, en Colombia, fue víctima de un ataque de *ransomware* en marzo de 2024 que comprometió la totalidad de su infraestructura digital, obligando a activar protocolos manuales de emergencia durante más de 48 horas (*La Patria*, 2024). En ambos casos, la ausencia de un enfoque preventivo desde el nivel directivo jugó un papel clave en la magnitud del impacto.

El otro gran reto, que no podemos dejar de lado, es el déficit de talento con las competencias indicadas en este aspecto. La Organización Mundial de la Salud (OMS) estima que, para el año 2030, habrá una escasez global de entre 10 y 18 millones de profesionales sanitarios con competencias digitales avanzadas (OMS, 2016). Esta brecha también afecta a los responsables de seguridad en salud digital, quienes muchas veces son roles compartidos o inexistentes en los hospitales públicos y privados de la región.

Además, el auge de dispositivos médicos conectados (IoMT) ha abierto una nueva puerta de entrada para los ciberatacantes. Según el estudio de Cynerio y Ponemon Institute (2022), el 43 % de los hospitales encuestados experimentaron incidentes cibernéticos directamente relacionados con dispositivos médicos conectados, comprometiendo funciones críticas como bombas de infusión y monitores de signos vitales.

En definitiva, el ciberataque es una realidad latente y se encuentra dentro de la actividad diaria de los centros de salud, pero ¿qué podemos hacer para mitigar estos riesgos desde la dirección?

> “El sector salud es hoy uno de los blancos principales de los ataques tipo *ransomware*”

Una tendencia cada vez más frecuente que han estructurado hospitales de alto impacto y con mayores riesgos, es la formación de los comités de ciberseguridad que reporten a la Dirección Médica y a la Gerencia de Calidad para el monitoreo constante de esos riesgos. Otra medida, es la adopción de normas como la ISO 27001 e ISO 27799, alineadas al Esquema Nacional de Seguridad (ENS) o Directiva NIS 2 sobre seguridad de las redes y de la información, según jurisdicción.

En el plano más operativo y directo ante la atención, se pueden diseñar planes de continuidad asistencial que contemplan trabajo “*offline*” seguro, como medidas de contingencia y hacer escenarios de simulacros para mejor adaptación por parte de los colaboradores. Crear alianzas estratégicas con centros de tecnología y universidades que desarrollen programas que permitan crear barreras accesibles. Y evidentemente, asignar un presupuesto del gasto en TIC destinado para esta finalidad. La ciberseguridad no es un gasto adicional ni un asunto exclusivo del

departamento de TI; es una dimensión crítica de la seguridad del paciente y la sostenibilidad financiera.

Para finalizar, quiero llamar a la reflexión de si como gestores de centros de salud estamos haciéndonos estas preguntas. ¿Estamos evaluando la ciberseguridad con el mismo rigor con que medimos la mortalidad o las infecciones nosocomiales? ¿Qué alianzas público privadas, académicas y tecnológicas podemos activar hoy para cerrar la brecha de talento mañana? Y, en última instancia, ¿cuánto riesgo residual estamos dispuestos a transferir a nuestros pacientes y comunidades cada día que postergamos la inversión en resiliencia digital? Debemos cuestionarnos constantemente para poder crear respuestas ajustadas a la realidad que estamos viviendo.

Bibliografía

1. Boletín Oficial del Estado. (2022). Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad . https://www.boe.es/eli/es/rd/2022/05/03/311

2. Instituto Cynerio y Ponemon (2022). Inseguridad de los dispositivos conectados en la atención médica 2022. https://cynerio.com/resources/insecurity-of-connected-devices-in-healthcare

3. El País. (2023, 6 de marzo). El Hospital Clínic de Barcelona sufre un ciberataque que paraliza su actividad. https://elpais.com/espana/catalunya/2023-03-05/el-hospital-clinic-de-barcelona-victima-de-un-ciberataque-que-afecta-a-las-urgencias-el-laboratorio-y-la-farmacia.html

4. La Patria. (2024, 19 de marzo). Hospital Universitario de Caldas activó plan de contingencia por ataque informático. https://www.lapatria.com/salud/software-malicioso-deja-en-urgencias-al-hospital-de-caldas-la-entidad-se-recupera

5. Organización Mundial de la Salud (OMS). (2016). Estrategia Global de Recursos Humanos para la Salud: Fuerza Laboral 2030 . https://www.who.int/publications/i/item/9789241511131

6. Sophos. (2024). El estado del *ransomware* en el sector sanitario 2024. https://www.sophos.com/en-us/content/state-of-ransomware-in-healthcare

Directora Fundadora Gestionando Salud

dcamacho@gestionandosalud.com