Deloitte.

Together makes progress

El sector salud frente a la tormenta de ciberataques

Introducción

La salud, tradicionalmente concebida como un refugio de confianza y cuidado, se ha convertido en uno de los objetivos más codiciados del cibercrimen global. Cada hospital, clínica o aseguradora es hoy un ecosistema digital donde conviven expedientes médicos, dispositivos conectados y plataformas que sostienen la vida de millones de pacientes. Sin embargo, esa misma red interconectada que potencia la innovación es la que incrementa el riesgo de ataques cibernéticos cada vez más difíciles de contener. Los ciberincidentes —que pueden costar millones de dólares en sanciones, rescates y pérdida de reputación— se traducen también en diagnósticos retrasados, cirugías canceladas y vidas en riesgo.

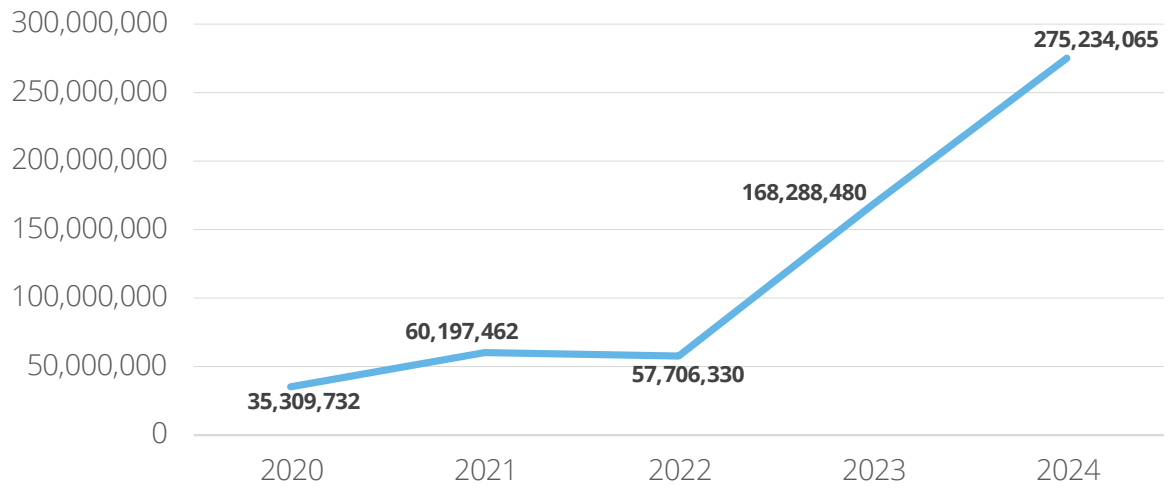
En este escenario, el sector salud no puede darse el lujo de esperar a que los gobiernos emitan regulaciones para reaccionar ante los riesgos, sino que debe anticipar, mitigar y transformar los riesgos antes de que se materialicen. La pregunta no es si ocurrirá un ataque, sino qué tan preparada está la organización para resistirlo y para mantener la operación, más aún cuando las amenazas evolucionan con rapidez, potenciadas por la inteligencia artificial y por cadenas de suministro interdependientes.

Por lo tanto, las organizaciones de salud están en un punto de inflexión: pasar de la reacción improvisada a la definición e implementación de estrategias integrales y sostenibles de ciberseguridad. Este punto de vista busca ofrecer una mirada clara y accionable sobre cómo enfrentar un desafío que trasciende lo técnico y se ha convertido en un asunto de confianza pública, continuidad clínica y competitividad en el sector.

El costo de las brechas de ciberseguridad en salud

El sistema de salud es un ecosistema altamente interconectado y en rápida transformación digital, lo que desafortunadamente lo convierte en un objetivo para actores maliciosos. Los hospitales, clínicas y aseguradoras manejan enormes volúmenes de datos sensibles y operan en entornos donde una interrupción puede, literalmente, costar vidas. En 2024, Estados Unidos vivió uno de los peores años registrados en brechas de datos de salud, con cifras que superan 275 millones de historiales clínicos expuestos[1], lo que representó un salto de 64% sobre el récord anterior. Solo un incidente —el ataque a una empresa de TI médica— comprometió la información de poco más de 190 millones de personas, convirtiéndose en la mayor brecha de salud de la historia[2]:

Registros médicos expuestos en brechas de seguridad en EE. UU.



Fuente: The HIPPA Journal.

El panorama de amenazas se agrava año tras año: en marzo de 2025, por ejemplo, 77% de las brechas en salud fue causado por ataques de hacking o incidentes de TI, los cuales, afectaron a 95% de los pacientes comprometidos en ese mes[3]. La magnitud y concentración de estos sucesos pudiera implicar que los incidentes son prolongados y sofisticados, y no necesariamente pérdidas accidentales o de errores puntuales.

La gravedad de estos incidentes queda ilustrada con casos concretos. En enero de 2025, un ataque de *ransomware* contra un hospital en Maryland, EE. UU., expuso los datos de poco más de 934 mil pacientes, robando información tan delicada como nombres, fechas de nacimiento, números de seguridad social, números de licencia, datos de seguro médico e información clínica sobre diagnósticos y tratamientos[4]. Este tipo de brechas, además de vulnerar la privacidad de los pacientes, deja a las organizaciones sanitarias enfrentando un dilema crítico: ver interrumpidos servicios esenciales. En todos los casos, es inmediato el daño reputacional y operativo, aunado a ello, se ve erosionada la confianza pública en el sistema de salud.

El impacto económico de las brechas de seguridad en salud es de grandes proporciones y va en ascenso. Según el Foro Económico Mundial, este sector ha reportado las pérdidas más grandes con respecto a incidentes en materia de ciberseguridad, los cuales costaron, en promedio, 10.93 mdd en 2023, manteniéndose como el sector con brechas más costosas por decimocuarto año consecutivo[5]. Si bien este promedio bajó ligeramente en 2024, aún duplica el promedio global de todos los sectores (4.88 mdd)[6]. De hecho, las brechas en salud superan por amplio margen a las del segundo sector más costoso, que es finanzas, con 6 mdd.[7]

La explicación radica en la riqueza de los datos médicos — un solo registro médico puede venderse en la *dark web* a un precio de entre 250 y 1,000 dólares, muy por encima de lo que puede valer, por ejemplo, una tarjeta de crédito robada— y en las severas consecuencias de paralizar la atención sanitaria, incluso, por poco tiempo. La cadena de costos de una brecha en salud abarca múltiples componentes, entre otros:

- **Detección y contención lentas:** en 2024, tomó 258 días, en promedio, detectar y contener una brecha (casi 9 meses de permanencia del intruso en los sistemas)[8]. Este prolongado tiempo de permanencia implica que el atacante puede maximizar el daño, antes de ser expulsado.

- **Pérdida operativa:** a menudo, las intrusiones provocan la suspensión de cirugías, consultas y servicios de diagnóstico, ralentizan investigaciones clínicas y ensayos, impiden un seguimiento adecuado de pacientes crónicos y causan caos en la facturación y tramitación de seguros. Cada día de interrupción supone retrasos en la atención y potenciales pérdidas de vidas o empeoramiento de pronósticos médicos.

- **Reputación y sanciones:** después de una brecha, las organizaciones enfrentan multas regulatorias y deben invertir en campañas de recuperación de la confianza. Además, no es raro ver demandas colectivas por parte de pacientes afectados, lo que añade costos legales significativos.

- **Recuperación y compensaciones:** restaurar sistemas y reforzar la seguridad con urgencia conlleva gastos enormes en personal técnico y en nuevo *hardware/software.* Adicionalmente, las entidades suelen costear servicios de monitoreo crediticio y protección de identidad para los pacientes cuyos datos fueron expuestos, asumiendo estos costos por años.

Una sola brecha con éxito puede suponer pérdidas directas e indirectas de millones de dólares. No es casualidad que los delincuentes busquen extorsionar al sector salud con demandas de rescate cada vez mayores: saben que "el tiempo de inactividad es muy lucrativo allí". Empero, el pago a ciberdelincuentes puede constituir una violación directa a las leyes de prevención de lavado y financiamiento ilícito, al representar un flujo monetario sin trazabilidad hacia estructuras criminales. Más allá de las sanciones legales, este tipo de pago erosiona la confianza pública y profundiza la vulnerabilidad de un sector esencial, donde la disponibilidad de datos clínicos puede ser una cuestión de vida o muerte.

La vulnerabilidad digital como amenaza a la atención médica

Cuando la ciberseguridad falla en un entorno sanitario, las consecuencias trascienden lo financiero y afectan directamente a la seguridad del paciente. Diversos análisis han establecido una preocupante cadena de causa-efecto: después de sufrir un ciberataque serio, los hospitales suelen ver degradado su desempeño clínico durante meses. Por ejemplo, un estudio sobre hospitales estadounidenses halló que luego de una brecha, la mortalidad a 30 días por infarto agudo de miocardio aumentó entre 0.23 y 0.36 puntos porcentuales, borrando muy rápido aproximadamente un año de avances en reducción de mortalidad[9]. Esta mayor mortalidad no se debe al ataque en sí, sino a los atrasos y dificultades operativas que se generan tras el incidente. En la práctica, esto significa diagnósticos tardíos, tratamientos pospuestos y una atención subóptima que pone en riesgo la vida de pacientes críticos.

Los ataques informáticos pueden dejar fuera de servicio equipos y sistemas esenciales. Imaginemos hospitales sin acceso a historiales electrónicos: cirugías que se cancelan, pacientes enviados a otros centros en ambulancia, médicos arriesgando medicar incorrectamente por desconocer alergias. Son situaciones que han pasado de la teoría a la realidad. En 2020, durante un ataque de *ransomware* al Hospital Universitario de Düsseldorf, en Alemania, una mujer murió al ser desviada 30 km a otro hospital porque la unidad de emergencias no podía atenderla a tiempo[10]. De forma similar, en Alabama, EE. UU., se atribuyó la muerte de un recién nacido a las fallas en monitores fetales durante un ataque de *ransomware* en 2019. Son ejemplos extremos, pero ilustran que la disrupción digital en salud tiene una conexión directa con la salud física de las personas.

Pero no solo los hospitales públicos son el objetivo de criminales; cualquier entidad sanitaria es vulnerable. Un caso sonado fue el de SingHealth en Singapur, en 2018, cuando un ciberataque robó 1.5 millones de registros (incluyendo los del Primer Ministro)[11]. Las investigaciones revelaron una serie de fallas en materia de ciberseguridad, pues un parche crítico nunca se aplicó, lo que habría prevenido la intrusión; además, el personal no estaba entrenado para reconocer ataques en curso, no escaló las alertas por temor y consideraba la seguridad "un asunto de TI". Esta combinación de vulnerabilidades técnicas y humanas permitió a los atacantes moverse con libertad y fugar datos sensibles durante meses sin ser detectados. El resultado no fue solo una multa para SingHealth, sino una pérdida masiva de confianza del público en el sistema de salud y un llamado de atención nacional sobre la necesidad de elevar los estándares de seguridad y de gobernanza.

Un nuevo rostro del cibercrimen en salud impulsado por IA

El panorama de amenazas cibernéticas contra la salud no deja de evolucionar, con vectores tanto tradicionales como novedosos, potenciados por nuevas herramientas (especialmente la inteligencia artificial), destacando los siguientes:

- ***Ransomware* "industrializado".** Los ataques de secuestro de datos han aumentado exponencialmente –278% en los últimos cinco años–[12], convirtiéndose en la pesadilla número uno del sector. Grupos criminales lanzan campañas de *ransomware* cada vez más agresivas, enfocándose en cifrar historiales y exigir millonarios rescates con la certeza de que muchas organizaciones sanitarias preferirán pagar para reanudar la atención al paciente.

- **Errores de configuración en la nube/híbrida.** La migración acelerada a la Nube ha expuesto nuevos flancos. Según una encuesta de ClearDATA, 80% de las entidades de salud sufrió al menos una configuración incorrecta en la Nube, en el último año[13] —ya sea un servidor con acceso público inadvertido, credenciales por defecto, ausencia de cifrado o políticas laxas. Este tipo de fallos es muy grave: la mayoría de las brechas se origina en configuraciones erróneas básicas que los atacantes explotan con facilidad. En otras palabras, la prisa por innovar sin las debidas protecciones está dejando puertas traseras abiertas.

- ***Phishing* potenciado por inteligencia artificial (IA).** La llegada de modelos generativos (*GPT*) ha revolucionado el *phishing*. Hoy, los delincuentes pueden generar, en minutos, miles de correos altamente personalizados y convincentes, adaptando idioma y contexto de la víctima, incluso, clonando voces o rostros mediante *deepfakes* para engañar en llamadas o videoconferencias. ¿El resultado? Ataques más verosímiles y difíciles de detectar. Un reciente experimento mostró que los correos fabricados con IA lograron que más de 30% de los destinatarios hiciera clic en enlaces maliciosos —superando con creces las tasas habituales de campañas manuales[14]. Con estas técnicas, el clásico correo de "su factura adjunta" se transforma en un mensaje prácticamente indistinguible de uno legítimo, venciendo filtros y engañando, incluso, a personal capacitado.

- **Cadena de suministro comprometida y *bots* maliciosos.** Los atacantes explotan cada vez más los eslabones débiles de terceros. Proveedores de TI, servicios de facturación, *softwares* de laboratorio, cualquier aliado tecnológico puede ser puerta de entrada. De hecho, se insiste en mapear y auditar la cadena digital de suministro precisamente porque un proveedor *hackeado* puede contagiar a decenas de clínicas[15]. En paralelo, prolifera el uso de redes de *bots* automatizados para amplificar ataques: programas maliciosos que imitan tráfico legítimo, pero en realidad, ejecutan robo de credenciales, raspado de datos de portales de pacientes o bombardeos de denegación de servicio. Estos *bots* apuntan tanto a infraestructuras de salud expuestas en internet como a *API* (Interfaz de Programación de Aplicaciones) y aplicaciones móviles, buscando cualquier resquicio para robar información o colapsar sistemas.

- **Amenazas habilitadas por IA clonable.** La inteligencia artificial no solo asiste a los defensores, también empodera a los atacantes. Herramientas de IA generativa permiten clonar identidades digitales y físicas, facilitando fraudes complejos. Hoy, es posible reproducir la voz de un médico o de un directivo con muestras mínimas, o generar videos falsos plausibles, y utilizar eso para engañar a empleados (por ejemplo, ordenando una transferencia de datos o deshabilitando un sistema de seguridad). Asimismo, la IA puede automatizar la búsqueda de vulnerabilidades en dispositivos médicos o sistemas heredados, a una velocidad antes inimaginable.

Regulaciones y exigencia creciente en el sector

Frente a los riesgos sistémicos, los reguladores internacionales están endureciendo las exigencias de ciberseguridad para las organizaciones de salud, conscientes de que la protección de los datos personales y la continuidad de servicios críticos no pueden quedar al azar.

Por ejemplo, entre 2022 y 2023, Australia sufrió brechas gigantescas que sacudieron al país. En particular, el *hackeo* a una importante aseguradora de salud expuso los datos de 9.7 millones de personas y reveló fallas básicas como la ausencia de autentificación multifactor (*MFA*, por sus siglas en inglés) en accesos remotos[16]. La reacción regulatoria ha sido firme: la Autoridad Australiana de Regulación Prudencial (*APRA*, por sus siglas en inglés) impuso a la empresa la obligación de apartar 167 mdd en capital extra, como protección por sus debilidades de seguridad, un castigo financiero inédito orientado a forzar mejoras rápidas.

De forma paralela, el gobierno federal elevó las multas por violaciones de privacidad y creó, en 2023, una agencia específica de ciberseguridad para coordinar respuestas nacionales. Ahora, el sector asegurador y de proveedores médicos en Australia enfrenta auditorías más frecuentes, y se espera la promulgación de normas que obliguen a terceros —como empresas de laboratorio o clínicas privadas— a notificar incidentes y cumplir estándares equivalentes a los de entidades públicas.

Otra tendencia surge en Estados Unidos con la actualización de la L*ey de Portabilidad y Responsabilidad de Seguros Médicos* (*HIPAA*, por sus siglas en inglés). El Departamento de Salud ha propuesto reforzar la norma con controles muy específicos y obligatorios. Entre los cambios planteados, están el cifrado obligatorio de la información clínica tanto en tránsito como en reposo, la autenticación multifactor en todos los sistemas que manejan datos de salud, la segmentación de la red para aislar sistemas críticos, escaneos periódicos de vulnerabilidades, así como auditorías anuales de cumplimiento en ciberseguridad.

Estas medidas buscan mitigar riesgos no atendidos en la normativa actual, pero vienen acompañadas de un costo considerable: se estima que el cumplimiento de estas nuevas reglas supondría unos 9 mil mdd en el primer año para el sector, y alrededor de 6 mil mdd anuales en los siguientes[17]. No resulta extraño el debate generado: hay quienes argumentan que, si bien necesarias, estas exigencias podrían desbordar a muchas entidades con recursos limitados, por lo que se aboga por enfoques escalonados y apoyo gubernamental para su implementación.

La Unión Europea sigue a la vanguardia con el *Reglamento General de Protección de Datos* (*GDPR*, por sus siglas en inglés) que, si bien no es sectorial, impone fuertes obligaciones de seguridad y protección de los datos a cualquier entidad que trate datos de salud de ciudadanos europeos. Adicionalmente, países europeos están fortaleciendo lineamientos específicos para infraestructuras críticas sanitarias (por ejemplo, la directiva NIS2). En Latinoamérica, países como Brasil, México, Argentina, Colombia y Chile han aprobado o actualizado leyes de protección de datos personales que incluyen a la salud como categoría sensible, requiriendo consentimientos explícitos, notificación de brechas y fijando sanciones civiles y penales por filtraciones. Si bien la madurez regulatoria varía, la tendencia regional es converger hacia estándares tipo *GDPR*.

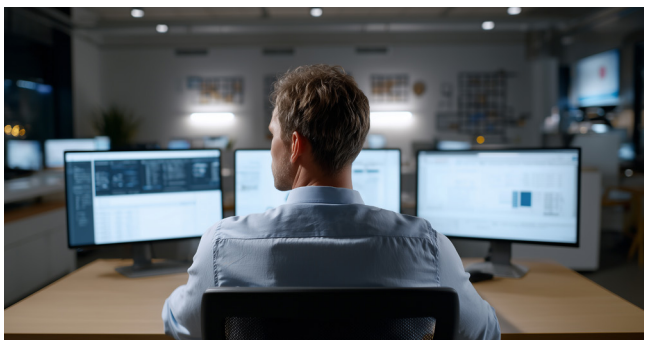
No obstante, el sector salud no debería esperar a que los gobiernos emitan nuevas regulaciones para reaccionar ante las crecientes ciberamenazas. La velocidad a la que evolucionan los ciberataques es vertiginosa, y cada día de inacción multiplica el costo potencial y la exposición al riesgo. Cada uno de los casos señalados con anterioridad subrayan un hecho incuestionable: la regulación siempre llega tarde, típicamente después de que los hechos consumados y las crisis ya han ocurrido. Quienes esperan una norma oficial para actuar confunden el simple cumplimiento regulatorio con una gestión estratégica del riesgo, exponiéndose a sufrir daños que ninguna ley posterior podrá deshacer.

Estrategias integrales que fortalecen la resiliencia digital en salud

Si cumplir normas no basta, ¿qué implica una estrategia integral de ciberseguridad para una organización de salud? Implica pasar de una mentalidad reactiva a una proactiva, incorporando la gestión de riesgos en la planificación estratégica de la institución. No se trata solo de comprar *firewalls*, sino de incorporar la seguridad como un proceso continuo y multidimensional. A grandes rasgos, un plan director de ciberseguridad en salud debería incluir los siguientes componentes:

1. **Diagnóstico y gestión de riesgos:** realizar una evaluación exhaustiva de la postura de ciberseguridad actual, identificando los puntos vulnerables. Esto implica mapear todos los sistemas, aplicaciones y flujos de datos (incluyendo equipos médicos conectados y expedientes clínicos), y puntos de falla críticos. Un análisis de riesgos periódico permite priorizar inversiones donde más afecta un incidente. Con base en ello, definir un plan de mejora alineado a marcos reconocidos y a los requerimientos regulatorios aplicables.

2. **Cultura de ciberhigiene y capacitación continua:** el eslabón humano sigue siendo el más débil en seguridad, pero también el más transformable. Invertir en concientización y formación recurrente del personal —tanto médico, como administrativo y técnico— para reconocer amenazas es una de las defensas más costo-eficientes. Una fuerza laboral vigilante puede prevenir incidentes antes de que ocurran, un esfuerzo sin costo relativo, en comparación con cualquier otra medida. La capacitación debe volverse parte del ADN institucional, con simulacros (por ejemplo, campañas de *phishing* simulado) y métricas de mejora.



3. **Gestión robusta de accesos e identidades:** controlar quién accede a qué, es fundamental en entornos con muchos empleados, terceros y dispositivos. Implementar *Single Sign-On* (inicio de sesión único) y autenticación multifactor para todos los usuarios, establecer control de accesos basado en roles (*RBAC*, por sus siglas en inglés) (nadie debería tener más privilegios de los necesarios), y monitorear activamente los accesos. Esto reduce drásticamente el riesgo de que credenciales robadas se utilicen para penetrar profundo en la red.

4. **Programa integral de privacidad de datos:** más allá de la seguridad técnica, las instituciones deben reforzar la gobernanza de datos personales. Esto incluye minimizar la recolección y retención de datos sensibles (si no lo tengo, no me lo pueden robar), clasificar la información según criticidad, y cifrar o seudonimizar datos siempre que sea posible. Un programa de privacidad debe asegurar cumplimiento legal (consentimientos adecuados, acuerdos de confidencialidad con terceros, políticas claras para pacientes) y tener preparado planes de notificación en caso de brecha.

5. **Segmentación de redes y aislamiento de sistemas críticos:** adoptar la filosofía de *Zero Trust* dentro de la red hospitalaria. Esto implica separar redes por función (clínica, administrativa, invitados), aislar equipos médicos y de *IoT* en subredes vigiladas, y aplicar filtros internos para que un atacante que comprometa un punto de acceso no tenga vía libre al resto. Del mismo modo, mantener copias de seguridad fuera de línea y segmentadas —para que un *ransomware* no cifre también las copias. La contención de cualquier incidente depende, en gran medida, de cuánto puede moverse lateralmente el intruso; con segmentación estricta, ese movimiento se limita o se detecta a tiempo.

6. **Resiliencia operativa y planes de contingencia:** asumir que eventualmente ocurrirá una brecha o caída, y prepararse para operar en modo degradado sin caos. Esto conlleva tener planes de continuidad de negocio específicos: desde poder regresar temporalmente a procesos en papel —como formularios de admisión manual o copias físicas de protocolos de emergencia—, hasta contar con sistemas de respaldo para funciones críticas. Los ejercicios de simulación son vitales: por ejemplo, desconectar deliberadamente la red de un área y medir si el personal puede seguir atendiendo pacientes apegado a los procedimientos de contingencia. La meta es que, aunque haya una interrupción, su efecto en la seguridad del paciente sea mínimo y controlado.

7. **Inversión en defensa basada en IA y automatización:** así como los atacantes usan IA, las organizaciones deben usarla para anticiparse. Existen herramientas de detección y respuesta automatizada (*EDR/XDR*, por sus siglas en inglés) potenciadas con inteligencia artificial que pueden identificar comportamiento anómalo en la red en tiempo real y neutralizar amenazas sin intervención humana. También, sistemas de análisis predictivo que alertan de vulnerabilidades antes de ser explotadas. Adoptar estas tecnologías reduce drásticamente el tiempo de respuesta y el error humano. Las empresas que suelen desplegar ampliamente IA y automatización en sus operaciones de seguridad experimentan ahorros significativos por brecha, además de acortar el ciclo de identificación y contención.

8. **Ciberseguros y simulacros activos:** considerar transferir parte del riesgo residual contratando ciberseguros; sin embargo, se debe tomar en cuenta que las aseguradoras están elevando sus exigencias, una póliza significativa solo es posible si la organización cumple ciertos estándares de seguridad. Además, un seguro no reemplaza la capacidad de respuesta interna. Es prudente realizar ejercicios de *red team/blue team* contratando expertos externos que intenten penetrar los sistemas (de forma controlada) para probar las defensas y la capacidad de detección del equipo interno. De igual manera, ejercicios de mesa *(table-top)* con la alta gerencia para ensayar cómo se tomarían decisiones bajo distintos escenarios (¿cuándo desconectar qué sistemas?, ¿cómo comunicar a pacientes y prensa?). Estos entrenamientos preparan a la organización para reaccionar de forma coordinada y eficiente cuando ocurra un incidente real.

9. Alianzas público-privadas y enfoque sistémico: dado que la salud es un elemento crítico, los actores deben colaborar y no trabajar en silos. Participar en centros de intercambio de información de amenazas del sector, colaborar con fuerzas del orden y con autoridades sanitarias, puede marcar la diferencia. Por ejemplo, notificar un ataque de forma temprana, a la autoridad correspondiente, ahorra en promedio 1 mdd de costos, respecto a las organizaciones que no lo hacen, y aumenta la probabilidad de evitar pagar rescates.[18] Asimismo, hay gobiernos que están promoviendo equipos de respuesta nacional especializados en salud, y las empresas deben aprovechar esa sinergia. La ciberseguridad en salud debe verse como un ecosistema: si un hospital sufre algún incidente, tener acuerdos para derivar pacientes a otros; si una clínica detecta un nuevo tipo de *malware*, alertar a las demás. Solo con esta mentalidad colectiva, se podrá responder a amenazas que también operan a escala global.

Implementar estas medidas requiere de inversión y liderazgo, pero los datos indican que muchas organizaciones están rezagadas. Por ejemplo, la Agencia de la Unión Europea para la Ciberseguridad establece que solo 27% de las entidades de salud cuenta con un programa de defensa dedicado contra *ransomware*, a pesar de ser la principal amenaza (representó 54% de los ataques en 2023)[19]. Esta brecha de preparación es justamente la oportunidad para mejorar: los tomadores de decisión deben reconocer que la ciberseguridad es una prioridad estratégica muy importante y que deben asignar recursos alineados a dicha relevancia.

Asimismo, las medidas antes mencionadas, combinadas, potencian sus resultados. Un informe canadiense mostró que las organizaciones con estrategias de ciberseguridad proactivas (varias de las anteriores implementadas) lograron reducir 50% la probabilidad de sufrir un ataque consumado respecto a aquellas con enfoque meramente reactivo[20]. Es importante recordar que la seguridad efectiva es el conjunto orquestado de tecnología, procesos y personas preparadas estratégicamente para prevenir, detectar y responder ante las amenazas, de tal manera que se reduzca la probabilidad de ocurrencia de un incidente y/o se mitigue el impacto del mismo.

Conclusión

La industria de la salud se encuentra en una encrucijada: por un lado, abraza la digitalización, la interoperabilidad y tecnologías disruptivas como la IA para mejorar la atención; por otro lado, esa misma digitalización ha ampliado la superficie de ataque y ha expuesto viejas y nuevas vulnerabilidades que los ciberdelincuentes están sabiendo explotar.

En este contexto, la ciberseguridad no debe verse como un gasto tecnológico, sino como un pilar estratégico importante. Al final es mejor invertir en prevención, que enfrentar una brecha de ciberseguridad con las consecuencias que hemos mencionado y que pudiera tener.

La verdadera ventaja competitiva y garantía de la continuidad reside en anticipar los riesgos, no en perseguirlos a destiempo. Robustecer la ciberseguridad podría facilitar el cumplimiento regulatorio al incorporar controles de seguridad desde el diseño, lo que reduce riesgos de multas y sanciones.

En última instancia, la ciberseguridad en los sistemas de salud busca proteger vidas y brindar confianza: las instituciones sanitarias que se adelanten a la siguiente amenaza estarán en mejor posición para salvaguardar la información sensible y seguir cumpliendo su misión crítica de cuidar a las personas, pase lo que pase en el ámbito digital. La inacción, por el contrario, solo multiplica la exposición y la probabilidad de sufrir un ciberataque.

Referencias

[1] Alder, S. (2025). *"2024 Healthcare Data Breach Report"*. The HIPAA Journal. www.hipaajournal.com/2024-healthcare-data-breach-report

[2] Alder, S. (2025). *"Change Healthcare Increases Ransomware Victim Count to 192.7 Million Individuals"*. The HIPAA Journal. www.hipaajournal.com/change-healthcare-responding-to-cyberattack

[3] McCormack, M. (2025). *March 2025 Healthcare Data Breaches: Hacking Remains the Top Threat.* Compliance Group. compliancy-group.com/march-2025-healthcare-data-breaches/

[4] Alder, S. (2025). *"Ransomware Attack on Frederick Health Medical Group Affects 934,000 Patients".* The HIPAA Journal. www.hipaajournal.com/frederick-health-medical-group-ransomware-attack

[5] Tashi Ukyab, K. y Beato, F. (2024). *"Healthcare pays the highest price of any sector for cyberattacks — that's why cyber resilience is key"*. World Economic Forum. www.weforum.org/stories/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key

[6] Tashi Ukyab, K. y Beato, F. (2024). *"Healthcare pays the highest price of any sector for cyberattacks — that's why cyber resilience is key".* World Economic Forum. www.weforum.org/stories/2024/02/healthcare-pays-the-highest-price-of-any-sector-for-cyberattacks-that-why-cyber-resilience-is-key

[7] Southwick, R. (2024). *"Healthcare data breaches remain most expensive of any industry"*. Chief Heatlhcare Executive. www.chiefhealthcareexecutive.com/view/healthcare-data-breaches-remain-most-expensive-of-any-industry

[8] Alder, S. (2024). *"Average Cost of a Data Breach Rises to $4.88M; Falls to $9.77M in Healthcare".* The HIPAA Journal. www.hipaajournal.com/cost-healthcare-data-breach-2024

[9] Alder, S. (2019). *"Report Suggests Augmented Security Following a Data Breach Contributes to Increase in Patient Mortality Rate".* The HIPAA Journal. www.hipaajournal.com/report-suggests-augmented-security-following-a-data-breach-contributes-to-increase-in-patient-mortality-rate

[10] Tmzid. (2025). *Healthcare Data Breach Statistics for 2025.* Bright Defense. www.brightdefense.com/resources/healthcare-data-breach-statistics

[11] Alder, S. (2019). *"SingHealth Breach Investigation Reveals Catalogue of Cybersecurity Failures".* The HIPAA Journal. www.hipaajournal.com/singhealth-breach-investigation-reveals-catalogue-of-cybersecurity-failures

[12] Tmzid. (2025). *Healthcare Data Breach Statistics for 2025.* Bright Defense. www.brightdefense.com/resources/healthcare-data-breach-statistics

[13] Cleardata. (2024). *Healthcare Cybersecurity Industry Insights: Survey Findings and Expert Opinions.* www.cleardata.com/blog/healthcare-cybersecurity-industry-insights

[14] Align. (2025). *Artificial Intelligence Is Making Phishing Nearly Impossible to Detect.* www.align.com/blog/ai-is-making-phishing-impossible-to-detect

[15] Eddy, N. (2025). *"2025's Biggest Healthcare Cybersecurity Threats".* Health Tech Magazine. healthtechmagazine.net/article/2025/01/healthcare-cybersecurity-threats-2025-perfcon

[16] Jose, R. y Manekar, S. (2023). *"Australia regulator tells Medibank to set aside $167 million after data breach"*. Reuters. www.reuters.com/business/finance/australia-regulator-asks-medibank-set-aside-167-mln-after-data-breach-2023-06-26

[17] Tshedimoso, M. (2025). *"Industry pushback grows against HIPAA Security Rule proposal".* HIPAA Times. hipaatimes.com/industry-pushback-grows-against-hipaa-security-rule-proposal

[18] Alder, S. (2024). *"Average Cost of a Data Breach Rises to $4.88M; Falls to $9.77M in Healthcare"*. The HIPAA Journal. www.hipaajournal.com/cost-healthcare-data-breach-2024

[19] European Union Agency for Cybersecurity, (2023). ENISA Threat Landscape: Health Sector. ENISA. www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf

[20] Happier It. (2025). *"White Paper: The Cost of Cybersecurity Breaches—Protecting Canadian Businesses from Financial Devastation".* www.happierit.com/whitepaper/avoid-costly-breaches-with-our-cybersecurity-expertise

Contactos

Paula Álvarez
Socia | *Technology & Transformation | Cyber*
Deloitte S-LATAM
palvarez@deloittemx.com

Andrea Bernales Zapata
Socia | *Technology & Transformation | Cyber*
Deloitte S-LATAM
abernales@deloittemx.com

Deloitte.