Cómo pueden los MSP posicionarse en el sector sanitario, un mercado de alto crecimiento

Los riesgos de ciberseguridad en el sector sanitario son extremadamente altos. Si los sistemas fallan o si se producen tiempos de inactividad, el impacto para los pacientes podría ser devastador. Por desgracia, muchas organizaciones sanitarias tienen dificultades para gestionar la ciberseguridad de forma eficaz. Esto ofrece a los proveedores de servicios gestionados (MSP) una gran oportunidad de ofrecer sus servicios y consolidar así su crecimiento.

Los datos del informe Black Book Market Research de 2025 ilustran la magnitud del desafío:

68 %
de los proveedores sanitarios afirman que no pueden abordar los riesgos de ciberseguridad de forma adecuada por culpa de la falta de fondos.

60 %
Casi el 60 % de las organizaciones sanitarias declara dificultades para contratar y retener a profesionales de TI cualificados.

28 %
de las brechas de seguridad se deben a errores humanos, y las amenazas internas proceden principalmente del phishing.

Como resultado, la adopción de servicios de seguridad gestionados en el sector sanitario creció un 35 % entre 2024 y 2025, lo que supone un escenario especialmente favorable para los MSP.[1]

La necesidad de ir más allá de los servicios gestionados estándar

Los entornos clínicos dependen de sistemas que deben estar siempre operativos, como las historias clínicas electrónicas, las plataformas de imágenes médicas y las herramientas de monitorización de pacientes. Un fallo en cualquiera de estos sistemas afecta de forma directa a los pacientes. Los MSP pueden ir más allá del soporte de TI tradicional y convertirse en partners esenciales para mantener los sistemas críticos en perfecto funcionamiento y garantizar la continuidad clínica, la seguridad y el cumplimiento normativo.

Sin embargo, prosperar en el sector sanitario exige mucho más que servicios gestionados estándar. Los MSP deben ser capaces de gestionar requisitos normativos complejos, proteger sistemas médicos heredados y ofrecer tiempos de inactividad casi nulos en entornos donde cada minuto resulta crucial.

[1] Black Book Market Research, The Black Book of Healthcare Cybersecurity: 2025 Edition

Desafíos empresariales y tecnológicos

Triunfar en el sector sanitario no resulta sencillo. Prestar servicios a organizaciones sanitarias plantea una serie de desafíos que muchos proveedores quizá no conozcan. Los MSP se enfrentan a una combinación única de presión operativa, riesgos de seguridad y complejidad técnica.

El impacto de los tiempos de inactividad en la seguridad de los pacientes

Las organizaciones sanitarias no pueden tolerar interrupciones. Los fallos de los sistemas pueden retrasar tratamientos, forzar la derivación de pacientes a otros centros y alterar flujos de trabajo clínicos críticos. Además, los tiempos de inactividad resultan costosos. Según IBM, el coste medio de una fuga de datos para las organizaciones sanitarias es de 7,42 millones de dólares.[2] Los MSP deben ofrecer objetivos de tiempo de recuperación prácticamente inmediatos y una alta disponibilidad de forma constante.

Aumento de la superficie de ataque debido a los sistemas heredados

Los entornos sanitarios siguen dependiendo de infraestructuras heredadas y dispositivos médicos conectados. Para aplicar parches en muchos de estos sistemas, se debe interrumpir la atención médica, por lo que los MSP acaban siendo responsables de proteger tecnologías obsoletas y vulnerables.

El alto valor de los datos sanitarios para los ciberdelincuentes

La información sanitaria protegida se encuentra entre los datos más valiosos de la internet oscura y en los entornos criminales. Como resultado, las organizaciones sanitarias son objetivos prioritarios para el ransomware y el robo de datos. Por lo tanto, los MSP deben ofrecer protección avanzada y recuperación rápida.

Aumento de las amenazas de ransomware

Los ataques de ransomware dirigidos al sector sanitario siguen aumentando. El FBI indica que los incidentes de ransomware notificados por organizaciones sanitarias crecieron un 93 % entre 2024[3] y 2025.[4] Los atacantes aprovechan la urgencia inherente a las operaciones clínicas. Los MSP deben implementar una protección por capas que incluya prevención, detección y una recuperación fiable.

Entornos híbridos complejos

Los entornos de TI sanitarios abarcan sistemas in situ, plataformas en la nube y aplicaciones clínicas especializadas. Mantener una interoperabilidad segura entre sistemas como las historias clínicas electrónicas (EHR) y las plataformas de imágenes médicas añade una complejidad técnica considerable.

Fragmentación de herramientas e ineficiencia operativa

Muchos MSP dependen de varias herramientas desconectadas para las copias de seguridad, la gestión y la seguridad. Ese enfoque aumenta la carga operativa, genera brechas de visibilidad y reduce la eficacia de la respuesta durante los incidentes.

[2] IBM. (2025). Informe Cost of a data breach report 2025: The AI oversight gap. IBM & Ponemon Institute.

[3] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2024). 2024 Internet Crime Report.

[4] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2025). 2025 Internet Crime Report.

Desafíos operativos y del sector

Más allá de los obstáculos técnicos, trabajar con clientes del sector sanitario implica exigencias normativas y operativas estrictas.

Cumplimiento normativo y presión de auditoría

Los MSP deben cumplir requisitos de cumplimiento normativo muy estrictos y, en muchos casos, asumir responsabilidad legal. La preparación para auditorías y la documentación resultan críticas, aunque pueden requerir una ingente cantidad de recursos.

Integridad de los datos y problemas de confianza

Las organizaciones sanitarias deben garantizar la exactitud y la integridad de los datos clínicos. Los daños en los datos que pasan desapercibidos y los registros incoherentes pueden dar lugar a riesgos diagnósticos graves que los MSP deben mitigar.

Requisitos de rendimiento para imágenes médica y datos

Los sistemas de imágenes médicas generan conjuntos de datos masivos que deben estar siempre disponibles para acceder a ellos de forma inmediata. Los MSP deben diseñar arquitecturas híbridas que equilibren el rendimiento con un almacenamiento seguro.

Restricciones presupuestarias

Las organizaciones sanitarias suelen operar con presupuestos de TI limitados, a pesar de las crecientes exigencias de seguridad. Por esa razón, los MSP deben ofrecer niveles elevados de protección y optimizar los costes al mismo tiempo.

Una plataforma diseñada para MSP del sector sanitario

Para triunfar en el sector sanitario, los MSP necesitan una plataforma que ofrezca seguridad, protección de datos y eficiencia operativa en una única solución: Acronis Cyber Platform, que permite a los MSP proteger todo el entorno clínico, simplificar las operaciones y mejorar la rentabilidad.

Con Acronis Cyber Platform, los MSP pueden:

Garantizar la continuidad clínica

- Garantizar que los sistemas críticos permanezcan disponibles en todo momento gracias a la restauración instantánea y a tiempos de recuperación prácticamente inmediatos.
- Mantener el acceso a las historias clínicas electrónicas (EHR), los sistemas de imágenes médicas y los dispositivos de monitorización a pie de cama incluso durante incidentes de ciberseguridad.

Proteger todo el entorno sanitario

- Proteger plataformas modernas de la nube y sistemas médicos heredados con un único agente integrado.
- Reducir el riesgo en los endpoints, en las cargas de trabajo y en los dispositivos del internet de las cosas médicas (IoMT, por sus siglas en inglés).

Simplificar el cumplimiento normativo y la preparación para auditorías

- Automatizar los procesos de cumplimiento normativo mediante mapas de protección de datos e informes listos para auditoría.
- Pasar de servicios de TI básicos a ofertas de cumplimiento de alto valor.

Restauración de datos segura

- Permitir una recuperación libre de malware gracias a las funciones de recuperación segura.
- Analizar y limpiar los datos de las copias de seguridad antes de restaurarlos.

Reducir la complejidad y mejorar los márgenes

- Eliminar la fragmentación de herramientas al consolidar las copias de seguridad, la gestión y la seguridad en una única plataforma.
- Mejorar la eficiencia de los técnicos y aumentar la rentabilidad de los servicios.

Acronis Cyber Platform: funciones diseñadas para el sector sanitario

Acronis ofrece un conjunto integral de funciones diseñadas específicamente para los entornos sanitarios:

Plataforma unificada de ciberprotección: Acronis combina ciberseguridad, copias de seguridad, recuperación ante desastres y administración de endpoints en una única plataforma, lo que reduce la complejidad operativa y mejora la visibilidad.

Copias de seguridad y recuperación avanzadas: los MSP pueden proteger sistemas críticos mediante copias de seguridad basadas en imágenes, almacenamiento inmutable y recuperación rápida para entornos clínicos y de imágenes médicas.

Protección de endpoints y EDR: con las funciones de Detección y respuesta en endpoints (EDR), los proveedores de servicios pueden proteger estaciones de trabajo clínicas, servidores y endpoints remotos.

Cumplimiento normativo y protección de datos automatizados: Acronis Cyber Platform permite a los MSP identificar y proteger los datos médicos confidenciales mediante herramientas de descubrimiento automatizadas e informes centralizados para facilitar la preparación para auditorías.

Protección de Microsoft 365: dado que muchas organizaciones sanitarias utilizan esta popular suite de productividad, los MSP pueden garantizar la continuidad de Microsoft 365 y de otras herramientas de comunicación y colaboración, incluidos el correo electrónico, el almacenamiento de archivos y las plataformas de coordinación de pacientes.

Compatibilidad con sistemas heredados: los MSP pueden ampliar la protección a sistemas operativos antiguos y dispositivos médicos especializados sin necesidad de llevar a cabo actualizaciones disruptivas.

Copias de seguridad forenses e integridad de los datos: los proveedores de servicios pueden capturar datos forenses para investigar incidentes y garantizar la integridad de los registros mediante tecnologías de verificación basadas en blockchain.

La ventaja de Acronis Cyber Platform

A diferencia de otras soluciones ensambladas de forma poco integrada, Acronis ofrece una plataforma integrada de forma nativa con un único punto de gestión que permite a los MSP:

- Ofrecer ciberprotección completa en entornos sanitarios.
- Reducir la carga operativa y la fragmentación de herramientas.
- Mejorar los tiempos de respuesta y los resultados de recuperación.
- Ampliar su oferta hacia servicios de seguridad y cumplimiento normativo de alto valor.
- Aumentar los márgenes y ampliar sus servicios para el sector sanitario.

Con las funciones esenciales consolidadas en una única plataforma, los MSP pueden reducir costes y simplificar las operaciones, al tiempo que ofrecen la resiliencia que exigen las organizaciones sanitarias.

Empiece a posicionar sus servicios en el sector sanitario

Las organizaciones sanitarias necesitan partners de confianza para garantizar la continuidad, la seguridad y el cumplimiento normativo. Acronis Cyber Platform permite a los MSP aprovechar esta oportunidad con total confianza.

↘ Reserve una demostración para descubrir cómo Acronis respalda a los MSP que trabajan con clientes del sector sanitario

↘ Inicie una prueba y comience a ofrecer servicios resilientes de MSP para el sector sanitario hoy mismo

Acronis

Más información en acronis.com