Cómo los MSP pueden proteger y ampliar sus servicios para clientes del sector de fabricación

Introducción: los fabricantes son el blanco de los ataques

El sector de fabricación se encuentra en el punto de mira de los ciberatacantes y muchas organizaciones no están preparadas para defenderse. Aunque representa un problema significativo para los fabricantes, también supone una gran oportunidad para los proveedores de servicios gestionados (MSP).

Cualquier responsable de un entorno de tecnología operativa (OT) es consciente del elevado coste que pueden suponer los tiempos de inactividad. IBM informó además de que, en 2025, el coste medio de una fuga de datos en el sector industrial ascendió a 5,6 millones de dólares[2], lo que sitúa al sector de fabricación solo por detrás de la sanidad y los servicios financieros en coste total por filtración.

> Según IBM, el sector de fabricación es el que más atacan los ciberdelincuentes, y lo ha sido durante los últimos cinco años[1]. Más de una cuarta parte de todos los ciberataques se dirige a fabricantes, según los datos de IBM.

La oportunidad de la tecnología operativa para los MSP

Las organizaciones con entornos de OT no operan de la misma manera que otros entornos operativos. Muchas, especialmente en el segmento de las pymes, carecen de la experiencia interna necesaria para gestionar entornos convergentes de TI y OT. En entornos aislados de la red, en los que una planta lleva a cabo sus operaciones diarias de forma independiente del resto de la organización, es posible que no haya personal de TI.

Ahí es donde los MSP pueden aprovechar una oportunidad de gran valor estratégico. Los fabricantes necesitan la ayuda de los MSP para garantizar el tiempo de actividad, proteger los sistemas críticos y mantener el cumplimiento normativo. Sin embargo, para los proveedores de servicios, el éxito en el sector de fabricación exige mucho más que simplemente dominar los servicios tradicionales de TI.

Para prosperar en este sector, los MSP deben evolucionar desde operadores de TI estándar hasta convertirse en partners de confianza capaces de dar soporte a sistemas críticos para la producción, donde los tiempos de inactividad repercuten de forma directa en los ingresos, la seguridad y los compromisos de la cadena de suministro.

[1] IBM. (2026). X-Force Threat Intelligence Index 2026

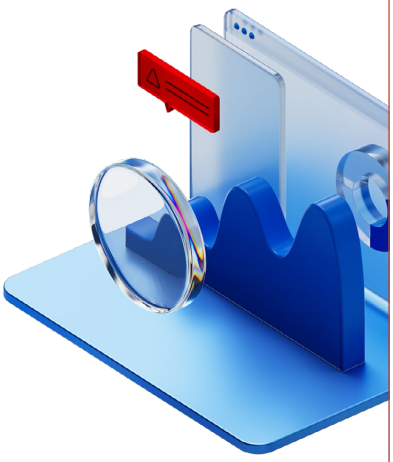
[2] IBM. (2025). Cost of a Data Breach Report 2025

Copyright © 2003-2026 Acronis International GmbH.

Principales riesgos en los entornos de fabricación

Lo primero que deben saber los MSP sobre la protección de las operaciones de OT es que los clientes del sector de la fabricación se enfrentan a una combinación única de riesgos empresariales y de ciberseguridad:

- **Tiempos de inactividad operativos:** incluso las interrupciones breves pueden detener las líneas de producción y provocar pérdidas financieras significativas.
- **Ataques de ransomware:** el sector de fabricación es uno de los objetivos prioritarios del ransomware debido al elevado coste de las interrupciones y al valor de los datos robados.
- **Interrupción de la cadena de suministro:** los incidentes de ciberseguridad pueden propagarse entre proveedores y partners, como demostró el ciberataque a gran escala de Jaguar-Land Rover en 2025.
- **Exposición de sistemas de larga vida útil:** los sistemas industriales diseñados para durar décadas pueden, por desgracia, aumentar la vulnerabilidad frente a ataques y limitar las opciones de aplicación de parches.



Riesgos derivados de la convergencia entre entornos de TI y de OT: la superficie de ataque se amplía a medida que los sistemas se interconectan.

Estos son los riesgos cuya mitigación permite a los MSP generar ingresos, siempre que dispongan de la plataforma correcta y del conocimiento adecuado para ello. Los MSP que prestan servicio a organizaciones con entornos de OT se enfrentan a una presión intensa para ofrecer no solo protección, sino también recuperación rápida de datos y continuidad operativa garantizada. Además, deben implementar sus servicios sin interrumpir la producción. En el sector de fabricación, no hay cabida para los tiempos de inactividad, que deben evitarse a toda costa.

Desafíos empresariales y tecnológicos

Existen varios aspectos clave que hacen que gestionar un entorno de OT resulte especialmente desafiante para los MSP.

Gestión de entornos híbridos complejos
Los entornos de fabricación combinan sistemas modernos de TI con tecnología operativa de larga vida útil, como los servidores de supervisión, control y adquisición de datos (SCADA), los controladores lógicos programables (PLC) y las interfaces hombre-máquina (HMI). Estos sistemas pueden resultar difíciles de actualizar, un problema persistente que puede abrir brechas de seguridad.

Visibilidad limitada entre TI y OT
Los MSP deben supervisar y proteger tanto las redes corporativas como los entornos de producción, pero la visibilidad entre ambos dominios suele estar fragmentada. Eso complica la detección y respuesta ante amenazas.

Aumento de la presión del ransomware
Los ciberdelincuentes atacan específicamente a los fabricantes debido a su baja tolerancia a los tiempos de inactividad. Los MSP deben garantizar funciones de prevención y recuperación rápida.

Herramientas fragmentadas y complejidad operativa
Muchos MSP dependen de varias herramientas individuales para las copias de seguridad, la supervisión y la seguridad. La fragmentación de herramientas incrementa los costes, ralentiza los tiempos de respuesta y genera desafíos de integración durante los incidentes.

Desafíos operativos y del sector

También existen desafíos y requisitos específicos en el sector de fabricación que los MSP deben afrontar y que no suelen encontrar en otros entornos, al menos no con la misma intensidad.

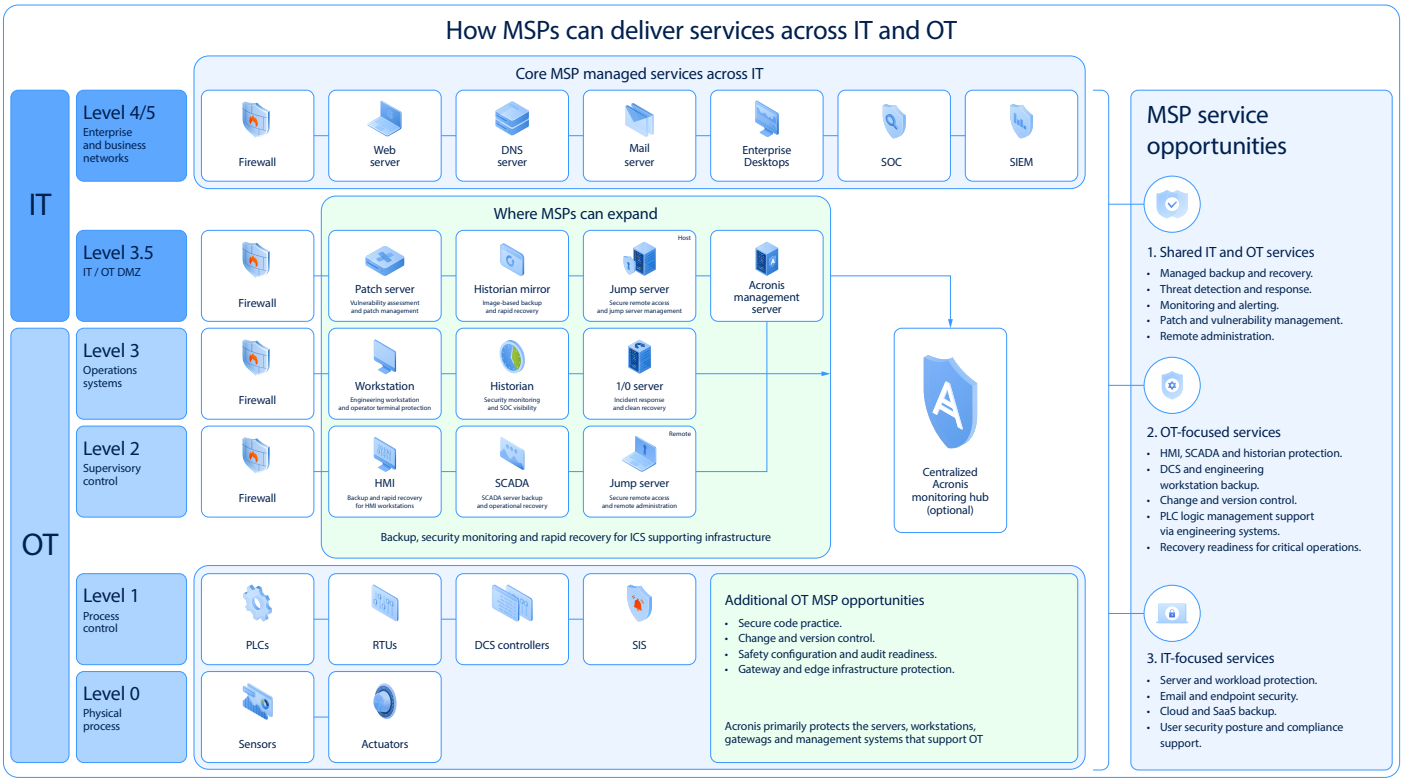
Requisitos estrictos de tiempo de actividad
Las operaciones de fabricación no pueden tolerar interrupciones. Los MSP deben ser capaces de cumplir objetivos de tiempo de recuperación muy exigentes y acuerdos de nivel de servicio (SLA) estrictos.

Sistemas heredados y limitaciones de los OEM
Los equipos industriales están diseñados para funcionar durante años, incluso décadas. Como resultado, a menudo utilizan sistemas operativos sin soporte o no admiten agentes de terceros debido a restricciones de garantía.

Presión normativa y de cumplimiento
Los fabricantes deben cumplir marcos como el NIST, el CMMC y las normas IEC, que exigen controles auditables y funciones de resiliencia.

Convergencia entre entornos de TI y de OT
Los MSP suelen iniciar su actividad en el sector de fabricación a través de servicios de TI y amplían progresivamente su alcance hacia los entornos de OT. Dar soporte a estaciones de trabajo de ingeniería, sistemas de historial de datos y sistemas HMI se convierte en un paso crítico para ofrecer el máximo valor. Los proveedores de servicios necesitan funciones específicas de OT si desean prosperar en el sector de fabricación.

Copyright © 2003-2026 Acronis International GmbH.



Solución: Acronis Cyber Platform

Acronis facilita la convergencia de la protección de TI y OT mediante una plataforma unificada que permite a los MSP proteger ambos tipos de entornos desde un único punto de control y garantizar la continuidad de la actividad empresarial. Con Acronis Cyber Platform, los MSP pueden:

Garantizar la continuidad de la producción con Acronis One-Click Recovery

Minimice los tiempos de inactividad con funciones integradas de copia de seguridad, ciberseguridad y recuperación casi instantánea. El personal técnico puede restaurar sistemas críticos en cuestión de minutos con un solo clic para mantener la producción en marcha.

Proteger la fábrica multigeneracional

Elimine la fragmentación de herramientas y proteja tanto las cargas de trabajo modernas en la nube como los sistemas industriales heredados desde una única plataforma integrada de forma nativa, sin interrumpir las operaciones.

Simplificar las operaciones y mejorar la eficiencia

Sustituya varias herramientas por una plataforma integrada para las copias de seguridad, la aplicación de parches, la supervisión y la seguridad, lo que reduce la complejidad y mejora la prestación de los servicios.

Facilitar el cumplimiento normativo y refuerce la confianza en la cadena de suministro

Facilite el cumplimiento de los requisitos normativos mediante generación de informes centralizada, visibilidad de vulnerabilidades y documentación lista para auditorías.

Habilitar un proceso de validación sin riesgos con gemelos digitales

Pruebe parches y actualizaciones en entornos virtuales antes de instalarlos para evitar interrupciones en la producción.

Superar las limitaciones de los OEM con protección sin agente

Proteja los recursos críticos sin instalar software en sistemas sensibles, preserve las garantías del fabricante y minimice los tiempos de inactividad durante las implementaciones.

Copyright © 2003-2026 Acronis International GmbH.

Acronis Cyber Platform para MSP

Acronis Cyber Platform es una plataforma unificada e integrada de forma nativa que ofrece ciberseguridad, protección de datos, gestión de infraestructura, automatización de servicios e infraestructura en la nube desde un único punto de control. Permite a los MSP eliminar la fragmentación de herramientas y mejorar la productividad del personal técnico.

Acronis Cyber Platform ofrece:

Copias de seguridad y recuperación ante desastres

- One-Click Recovery, que permite a los MSP restaurar los sistemas con rapidez.
- Copias de seguridad inmutables para proteger frente al ransomware.
- Universal Restore para recuperar datos o sistemas independientemente del hardware.

Seguridad avanzada y XDR

- Protección frente al ransomware basada en IA.
- Detección y respuesta integradas en endpoints, correo electrónico y cargas de trabajo.

Administración avanzada y aplicación de parches

- Aplicación automatizada de parches con reversión a prueba de fallos.
- Evaluación de vulnerabilidades en sistemas que dan soporte a TI y OT.

Seguridad del correo electrónico y formación en concienciación

- Protección frente a ataques de phishing impulsada por IA.
- Formación específica para usuarios del sector de fabricación.

Además, Acronis Cyber Platform proporciona protección para infraestructuras críticas que dan soporte a sistemas de control distribuido (DCS), SCADA y HMI. En conjunto, estas funciones permiten a los MSP ofrecer una capa completa de resiliencia que complementa las herramientas existentes de supervisión de red y de OT.

Acronis Cyber Platform para MSP

La ventaja de Acronis para los MSP del sector de fabricación

A diferencia de otras soluciones que solo ofrecen copias de seguridad o funciones de seguridad, Acronis pone a disposición de los usuarios una plataforma unificada de ciberprotección diseñada para entornos complejos.

Este enfoque permite a los MSP:

- Reducir la carga operativa y eliminar la fragmentación de herramientas.
- Mejorar los tiempos de respuesta durante los incidentes.
- Centrarse en el tiempo de actividad y la resiliencia.
- Ampliar su alcance desde entornos de TI hacia entornos de OT con total confianza.

En definitiva, consolidar las funciones de protección en una única plataforma reduce los desafíos de integración y el riesgo operativo, además de mejorar la eficiencia global.

Dé el paso hacia el sector de fabricación

Los fabricantes necesitan el apoyo de los MSP, ya que buscan invertir en tiempo de actividad, resiliencia y continuidad de la actividad empresarial con partners de confianza. Acronis permite a los MSP aprovechar esa excelente oportunidad.

Empiece a posicionarse en el sector de fabricación hoy mismo

- Reserve una demostración de Acronis Cyber Platform.
- Inicie una prueba de Acronis Cyber Platform.

Acronis

Más información en acronis.com

Copyright © 2003-2026 Acronis International GmbH. Reservados todos los derechos. Acronis y el logotipo de Acronis son marcas comerciales de Acronis International GmbH en Estados Unidos y otros países. Todas las demás marcas comerciales o registradas son propiedad de sus respectivos propietarios. Nos reservamos el derecho a que haya cambios técnicos y diferencias con respecto a las ilustraciones; declinamos la responsabilidad por cualquier error (junio de 2026).