

Preservación del tiempo de actividad en entornos de tecnología operativa (OT)

Los elevados costes del tiempo de inactividad de los sistemas de OT

Los sistemas de tecnología operativa (OT) son un eslabón crítico para mantener el tiempo de actividad de la producción y la rentabilidad de las empresas. Cuando fallan, pueden arrastrar consigo líneas de montaje, oleoductos, redes de servicios públicos y cadenas de suministro. Los costes de las interrupciones resultantes pueden ascender a decenas o cientos de miles de dólares por hora. Una encuesta de ABB reveló que el 69 % de las empresas habían sufrido tiempos de inactividad una vez al mes, y que dichas interrupciones les suponían 150 000 \$ por hora¹. Entre otras de las consecuencias de sufrir tiempos de inactividad en sistemas de OT se incluyen las siguientes:

- Costes de oportunidad de ventas debido a pedidos no satisfechos y plazos de entrega más largos.
- Aumento de los costes laborales directos por cantidad de bienes producidos.
- Daño a la relación con los clientes y a la reputación de la marca causado por entregas lentas o incumplidas.
- Disminución de la capitalización bursátil a medida que los inversores pierden la confianza en la capacidad de la empresa para mantener una producción coherente.
- Sanciones económicas por infringir los acuerdos de nivel de servicio (SLA) u otras obligaciones contractuales.
- Multas o sanciones penales por no cumplir los requisitos normativos en materia de ciberresiliencia.

Por lo tanto, es primordial proteger los sistemas de OT frente a posibles ciberataques, desastres naturales, fallos de software o hardware y errores humanos, y volver a ponerlos en funcionamiento cuanto antes en caso de que ocurra alguno de estos incidentes.

Muchos sectores, como el de la automoción, la energía, el farmacéutico y el logístico, dependen en gran medida de la automatización de los procesos de producción en tiempo real. Gran parte de esa tecnología de automatización la controlan, configuran y supervisan ordenadores que ejecutan Windows o Linux y que se engloban en el ámbito de la tecnología operativa (OT), los sistemas de control industrial (ICS) y la infraestructura ciberfísica. Entre las aplicaciones de OT más comunes figuran los sistemas de supervisión, control y adquisición de datos (SCADA), los sistemas de control distribuido (DCS), las interfaces hombre-máquina (HMI) y los sistemas de historial operativo que capturan datos de procesos en tiempo real.

¹ ABB. [“Value of Reliability: ABB Survey Report 2023”](#).

Los desafíos de mantener el tiempo de actividad de los sistemas de OT

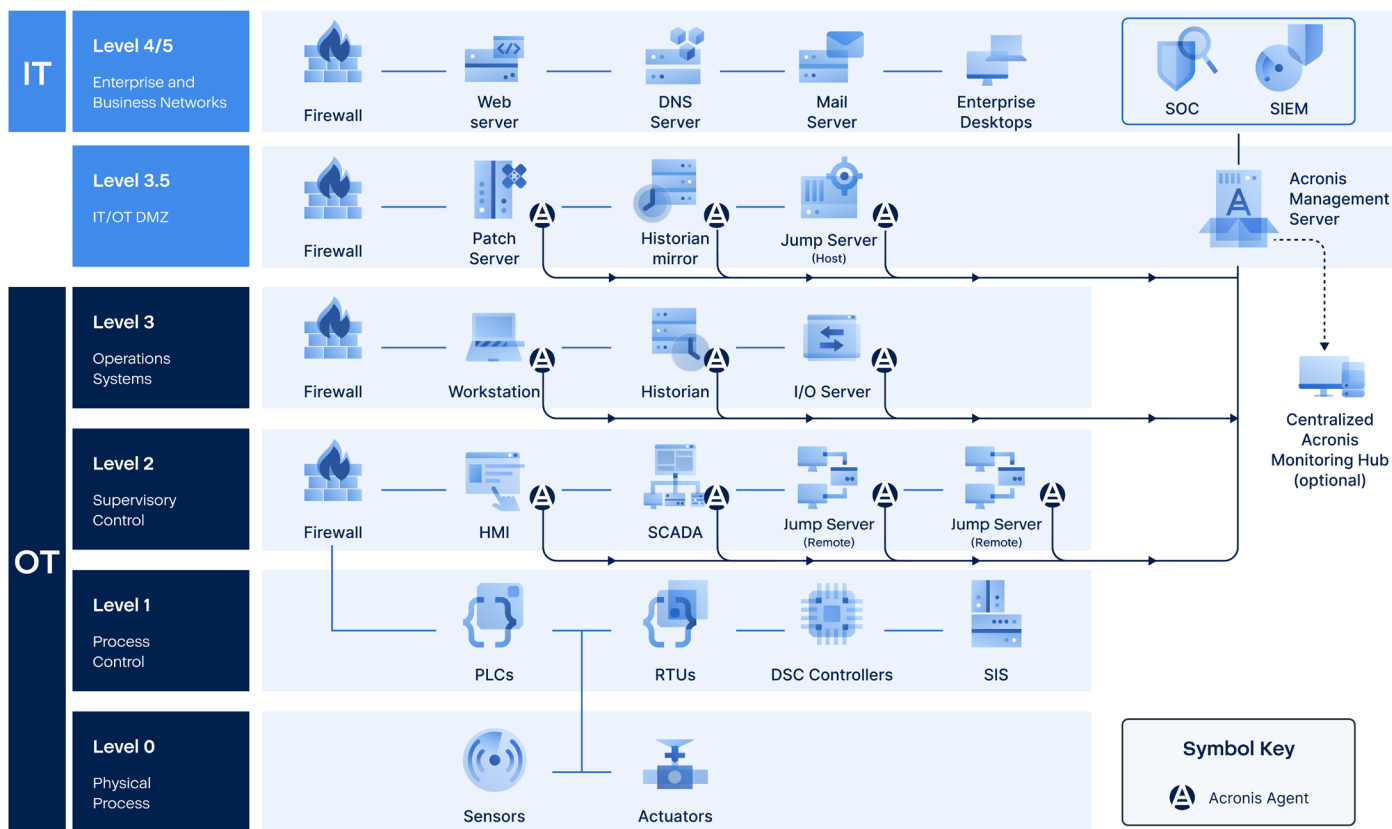
La presión por minimizar el tiempo de inactividad de los sistemas de OT se intensifica debido a las características únicas e inherentes de dichos sistemas, lo que hace que su mantenimiento y funcionamiento sean aún más complejos en comparación con los sistemas de TI tradicionales de administración interna (back-office) y de atención al público (front-office).

- Muchos sistemas de OT se ejecutan en hardware y sistemas operativos (SO) muy antiguos, algunos incluso de la época de Windows XP. Actualizarlos a nuevas revisiones de hardware y SO conlleva riesgos, ya que puede comprometer o limitar la funcionalidad de las aplicaciones de OT.
- La antigüedad de estos sistemas también dificulta o incluso impide equiparlos con medidas de ciberseguridad actualizadas, como la Detección y respuesta para endpoints (EDR).

- Cuando un proveedor de sistemas operativos anuncia la fecha de fin de soporte para una versión concreta de su producto (p. ej., como hizo Microsoft con Windows XP en abril de 2014), los principales proveedores de copia de seguridad suelen dejar de dar soporte a esa versión en un plazo de cinco años, y a menudo incluso antes. Sin el soporte de un buen proveedor de copias de seguridad, los ingenieros de OT se ven obligados a depender de procesos de copia de seguridad lentos, manuales y propensos a errores que requieren costosos tiempos de inactividad programados para ejecutarse.
- Las instalaciones donde se encuentran los sistemas de OT rara vez disponen de soporte de TI in situ y suelen estar lejos de los equipos de TI centralizados. Además, los entornos de OT suelen estar aislados para reducir los riesgos de ciberseguridad, lo que impide al equipo de TI utilizar herramientas de supervisión y gestión remotas. Desplazar físicamente al personal de TI a las instalaciones de producción puede llevar demasiado tiempo y ser muy costoso, lo que prolongaría las interrupciones y aumentaría considerablemente el gasto.

Acronis cumple con los requisitos de ciberresiliencia exclusivos de los entornos de OT

La plataforma Acronis Cyber Protect se utiliza ampliamente en el sector industrial y en el de la fabricación para proteger una gran variedad de sistemas de OT, incluidos, entre otros, los ejemplos del modelo Purdue que se muestran en la Figura 1.



*List of protected systems not exhaustive

Figura 1: Ejemplos de sistemas de OT protegidos por Acronis, según el modelo Purdue

Acronis Cyber Protect ofrece funciones de copia de seguridad y recuperación para sistemas de OT con funciones esenciales en entornos de producción que no solo requieren un tiempo de actividad extremadamente alto, sino también lo siguiente:

- La posibilidad de instalar el agente de Acronis Cyber Protect y realizar copias de seguridad sin necesidad de desconectar o reiniciar el sistema de OT.
- Ejecución de copias de seguridad rápida, fiable y totalmente automatizada que libera al sistema de OT de la sobrecarga que supone procesar y almacenar las copias de seguridad.
- La posibilidad de estandarizar (o personalizar) las copias de seguridad en todos los sistemas y ubicaciones con planes de protección de datos.
- Funciones de ciberseguridad opcionales que utilizan el mismo agente de Acronis, incluidas las de EDR, antimalware y antiransomware.

Acronis protege incluso los sistemas de OT más antiguos

Acronis refuerza la estabilidad de los entornos de OT al proteger todos los sistemas operativos desde la época de XP hasta la actualidad (incluidos los sistemas operativos que otros proveedores abandonaron hace tiempo). Esto garantiza que incluso los sistemas más antiguos se puedan recuperar de forma rápida y fiable, con la opción de replicar un sistema en nuevo hardware a través de un proceso denominado "recuperación desde cero", si fuera necesario. Esta función instala automáticamente los controladores nuevos necesarios para garantizar que el sistema operativo y las aplicaciones de OT se ejecuten correctamente en el nuevo hardware. En la Figura 2 se muestra el alcance del soporte de Acronis para sistemas operativos e hipervisores desde la época de XP hasta la actualidad, y a su vez se destacan las versiones de Windows y Linux más utilizadas en entornos de OT:

La mejor cobertura del sector para varios sistemas operativos e hipervisores

Windows

- Windows Server 2003 SP1, R2 y versiones posteriores, 2008, 2008 R2, 2012/2012 R2, 2016, 2019, 2022, excepto Nano Server
- Windows Small Business Server 2003/2003 R2, 2008, 2011
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows XP Professional SP1, SP2, SP3
- Windows 7, 8/8.1, 10, 11 (todas las ediciones, excepto Windows RT)

Microsoft SQL Server

2022, 2019, 2017, 2016, 2014, 2012, 2008 R2, 2008, 2005

Microsoft Exchange Server

2019, 2016, 2013, 2010, 2007

Hipervisores

VMware vSphere

4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Microsoft Hyper-V Server

2022, 2019, 2016, 2012/2012 R2, 2008/2008 R2

Citrix XenServer/Citrix Hypervisor

8.2-4.1.5

Linux KVM

7.6-8

Scale Computing Hypercore

8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV)

2.2-3.6

Red Hat Virtualization

4.0, 4.1, 4.2, 4.3, 4.4

Virtuozzo

7.0.14-6.0.10

Virtuozzo Infrastructure Platform

3.5

Nutanix Acropolis Hypervisor (AHV)

de 20160925.x a 20180425.x

MacOS

- **OS X** Mavericks 10.9, Yosemite 10.10, El Capitan 10.11
- **macOS** Sierra 10.12, High Sierra 10.13, Mojave 10.14, Catalina 10.15, Big Sur 11, Monterey 12, Ventura 13, Sonoma 14

Linux: Kernel entre 2.6.9 y 5.19

- RHEL 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10-23.04
- Fedora 11-31
- SUSE Linux Enterprise Server 10, 11, 12, 15
- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4-7.7, 8.0-8.8, 8.11, 9.0-9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.x*, Stream 8*, 9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

Figura 2: Soporte de Acronis para sistemas operativos e hipervisores

Acronis permite restaurar sistemas de OT sin que deba intervenir el equipo de TI

Acronis ofrece One-Click Recovery, una función exclusiva fundamental en entornos de OT que carecen de personal de TI in situ o que están aislados sin conexión a internet, lo que impide utilizar herramientas de administración remota por parte del personal de TI centralizado. Acronis One-Click Recovery permite a cualquier trabajador local, sin importar su experiencia en TI, recuperar un sistema de OT que haya fallado a partir de una copia de seguridad local con solo pulsar unas teclas. Las costosas interrupciones de la producción por culpa de fallos en los sistemas de OT, que pueden tardar horas o incluso días en resolverse, además del tiempo necesario para que el personal de TI se desplace a las instalaciones afectadas, se pueden reducir en cuestión de minutos. La función One-Click Recovery permite recuperar sistemas de OT desde una copia de seguridad en un disco local o en la nube de Acronis, y proteger las copias de seguridad con cifrado Bitlocker y contraseñas de recuperación.

Los principales proveedores de automatización utilizan la protección de sistemas de OT de Acronis

Los principales proveedores de tecnología operativa (OT) y de sistemas de control industrial (ICS), entre los que se incluyen ABB, Siemens, Honeywell, utilizan Acronis Cyber Protect como solución de copia de seguridad para sus clientes, como parte de una solución de marca blanca o de marca conjunta. Ningún otro proveedor de protección de datos disfruta de una gama similar de alianzas y recomendaciones por parte del sector de la automatización.

Acronis, líder en ciberresiliencia para sistemas de OT

Las principales empresas de investigación tecnológica, como Forrester Research, TAG Infosphere y Omdia, califican a Acronis como líder en protección de sistemas de OT.

[Informe de TAG Infosphere](#)[LEER](#)[Informe de Omdia](#)[LEER](#)

Conclusión

Acronis Cyber Protect se utiliza para proteger los sistemas de OT en entornos de fabricación y producción industrial de todo el mundo. Su exclusiva combinación de funciones, como las de protección de datos para sistemas operativos desde la época de XP hasta la actualidad y la herramienta One-Click Recovery, que permite a empleados sin conocimientos técnicos restaurar los sistemas afectados, junto con su adopción por parte de los principales proveedores de automatización, ha contribuido a que la comunidad de analistas reconozca a Acronis como líder en ciberresiliencia para sistemas de OT.



LECTURA ADICIONAL

Obtenga más información sobre Acronis Cyber Protect para sistemas de OT

[Soluciones de fabricación de Acronis](#)[Infografía: Mantenimiento del tiempo de actividad de sistemas de OT con One-Click Recovery](#)[Caso práctico: Productos derivados de Tata Steel](#)[Caso práctico: ABB](#)[Caso práctico: Johnson Electric](#)[Caso práctico: BDR Pharma](#)[Obtenga una prueba gratuita de Acronis Cyber Protect](#)[Hable con un especialista en ciberresiliencia para sistemas de OT](#)