Más allá de la ciberseguridad: desarrollo de la ciberresiliencia para garantizar la continuidad de la actividad empresarial

Por qué los líderes de TI modernos deben
prepararse para las interrupciones,
no solo para prevenirlas.

Ciberseguridad frente a ciberresiliencia

La ciberseguridad se centra en detener ataques. La ciberresiliencia, por su parte, garantiza la continuidad de la actividad empresarial durante y después de un ataque.

Ciberseguridad
Prevención, defensa perimetral, prevención de brechas de seguridad.

Ciberresiliencia
Adaptabilidad, recuperación, continuidad de la actividad empresarial.

Impacto de la continuidad de la actividad empresarial en diferentes sectores

Por qué la ciberresiliencia importa en los sectores críticos

El tiempo de inactividad y las interrupciones causadas por ciberataques afectan a todos los sectores, pero las consecuencias varían según el sector.

Sanidad

60 %

Porcentaje de organizaciones de atención sanitaria que señalan que los ciberincidentes interrumpen directamente la atención a los pacientes.[1]

Por qué es importante:
El tiempo de inactividad puede retrasar tratamientos, desviar a los pacientes y comprometer la seguridad.

Comercio minorista

43 %

Porcentaje de minoristas que experimentaron al menos una interrupción grave causada por incidentes de TI o ciberataques en el último año.[2]

Por qué es importante:
Incluso las interrupciones breves afectan a los ingresos, a la visibilidad del inventario y a la experiencia de los clientes.

Servicios financieros

91 %

Porcentaje de instituciones financieras que experimentaron al menos un ciberincidente en el último año.[3]

Por qué es importante:
El tiempo de inactividad afecta el procesamiento de transacciones, a la confianza de los clientes y al cumplimiento normativo.

Logística y transporte[4]

94 %

Porcentaje de organizaciones que afirman que las interrupciones causadas por ciberataques pueden provocar fallos en cascada en la cadena de suministro.[5]

Por qué es importante:
El tiempo de inactividad detiene el seguimiento de envíos, las operaciones del almacén y las entregas "justo a tiempo".

Administración pública

60 %

Porcentaje de interrupciones de red que cuestan a las organizaciones al menos 1 millón de dólares en interrupciones operativas.[6]

Por qué es importante:
Las interrupciones afectan a los servicios al ciudadano, a la respuesta ante emergencias y a la confianza pública.

El tiempo de inactividad es un fallo en la continuidad de la actividad empresarial

El tiempo de inactividad afecta a los ingresos, a las operaciones y a la reputación, no solo a los sistemas de TI.

96 %

Porcentaje de organizaciones que experimentó al menos una interrupción en los últimos tres años.

80 %

Porcentaje de organizaciones que aseguran que las interrupciones traen consigo consecuencias cada vez más graves.[7]

Por qué la redundancia tradicional falla frente al ransomware

La redundancia protege contra fallos de hardware, no contra ataques inteligentes y propagables.

La replicación puede propagar infecciones.

La fragmentación de las herramientas de recuperación ante desastres y de copia de seguridad genera puntos ciegos.

La fragmentación de herramientas aumenta el tiempo de recuperación y añade ineficiencia operativa.

La resiliencia moderna requiere nuevos parámetros de recuperación

La velocidad por sí sola no basta: la recuperación debe ser limpia y estar alineada con la empresa.

RTO	Tiempo máximo para restaurar operaciones
RPO	Pérdida de datos máxima aceptable
MTD	Tiempo máximo tolerable de inactividad antes de que el negocio falle
MTCR	Tiempo necesario para restaurar un entorno verificado y libre de malware

La recuperación limpia es ahora un requisito de continuidad

Recuperar rápidamente la continuidad de la actividad empresarial no tiene sentido si los sistemas restaurados están comprometidos.

- Coste medio de una fuga de datos: 4,45 millones de dólares.
- Las interrupciones operativas representan el componente de coste más elevado en las brechas de seguridad.[8]

Lo que los líderes de TI deben priorizar en el negocio

La resiliencia es una decisión económica y operativa.

Acciones prioritarias (de alto nivel)

- **Alinear la protección con la criticidad de los recursos.**
- **Probar la recuperación en escenarios reales de ciberataques.**
- **Validar las copias de seguridad antes de la restauración.**
- **Reducir la complejidad a través de plataformas unificadas.**

La ciberresiliencia permite mantener la continuidad, la confianza y el control, incluso cuando los ataques son inevitables.

De la ciberseguridad a la ciberresiliencia con Acronis

La ciberseguridad depende de algo más que la protección. Requiere resiliencia. Descubra cómo Acronis puede ayudarle a anticiparse a las amenazas, resistir los ataques, recuperarse más rápido de sus consecuencias y adaptarse de cara al futuro.

Contáctenos

---

[1] Departamento de Salud y Servicios Humanos de EE. UU. (HHS)
https://www.hhs.gov/about/news/2023/12/01/ransomware-cyber-attacks-threaten-patient-safety.html

[2] Uptime Institute. "Annual Outage Analysis 2023".
https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[3] Foro Económico Mundial. "Global Cybersecurity Outlook 2024".
https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

[4] Foro Económico Mundial: Global Risks Report
https://www.weforum.org/reports/global-risks-report-2024

[5] Ibid.

[6] Intelligent CIO. "US government organizations lose millions in an average network outage or breach".
https://www.intelligentcio.com/north-america/2021/01/26/us-government-organizations-lose-millions-in-an-average-network-outage-or-data-breach/

[7] Uptime Institute. "Annual Outage Analysis 2023".
https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[8] IBM. "Cost of a Data Breach Report 2025".
https://www.ibm.com/reports/data-breach