

Los nuevos KPI de la ciberresiliencia

Los parámetros tradicionales de recuperación miden la velocidad y la pérdida de datos. Sin embargo, las amenazas modernas requieren indicadores clave de rendimiento (KPI) que midan la ausencia de malware en los procesos de recuperación y el nivel de interrupción aceptable.

Por qué los KPI heredados son insuficientes

KPI heredados

RPO

Objetivo de punto de recuperación

Cuánta pérdida de datos es aceptable.

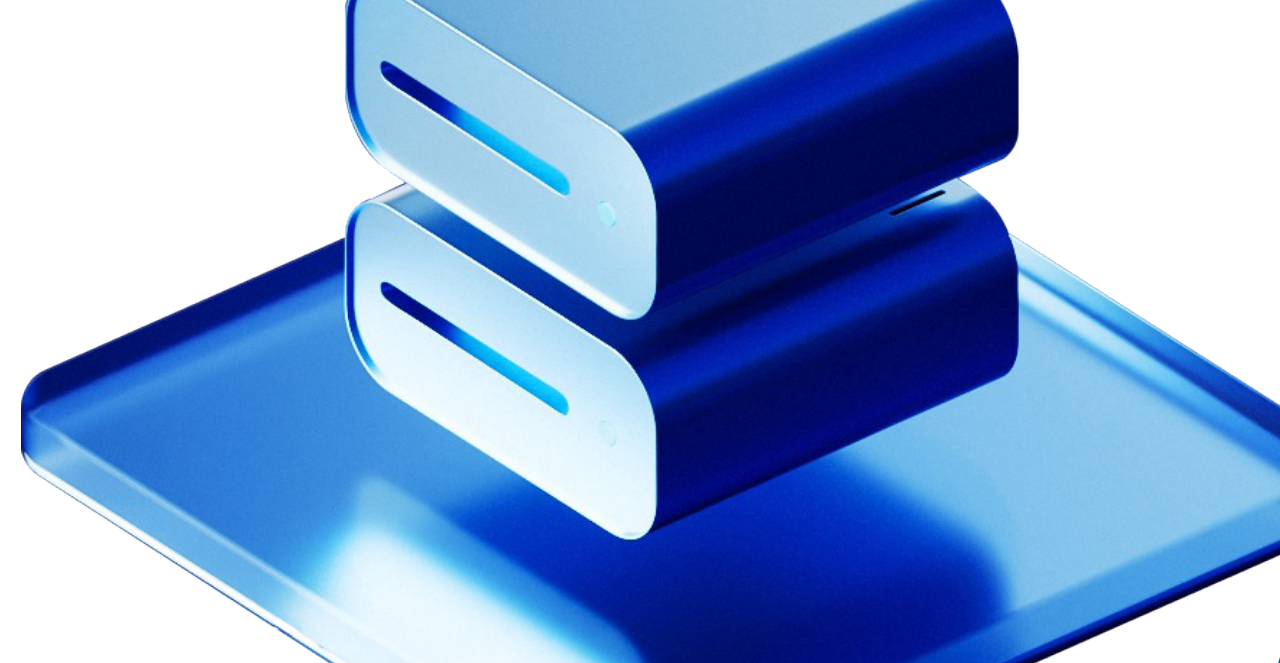
RTO

Objetivo de tiempo de recuperación

Con qué rapidez deben restaurarse los sistemas.

Una recuperación rápida que restaura un sistema infectado sigue siendo un fracaso.

Estos KPI se crearon para fallos de hardware e interrupciones por causas naturales. No contemplan ataques que comprometen la integridad de los sistemas.



Los KPI modernos: MTCR y MTD

KPI	MTCR	MTD
Nombre completo	Tiempo medio para una recuperación limpia.	Interrupción máxima tolerable.
Definición	El tiempo necesario para restaurar un entorno verificado, libre de malware.	El tiempo máximo que una empresa puede permanecer offline o en un estado degradado antes de que el impacto resulte inaceptable.
Por qué es importante	Garantiza que el sistema restaurado no esté comprometido y sea seguro de utilizar.	Alinea las decisiones de recuperación con el impacto en el negocio.

El modelo heredado frente al de resiliencia

Modelo heredado

RTO

RPO

Modelo de resiliencia

RTO

RPO

MTCR

MTD



La recuperación moderna exige tanto rapidez como fiabilidad.

El tiempo de inactividad destruye la productividad

23 días

Tiempo promedio de inactividad por ransomware.¹

76 %

Porcentaje de organizaciones que informan de una pérdida significativa de productividad tras sufrir un incidente.²

30 %

Porcentaje del tiempo que se dedica a responder ante interrupciones de TI al año.³

1,5-3 horas

Productividad que se pierde a diario debido a la fragmentación de herramientas.⁴

Los tiempos de inactividad y las pilas tecnológicas fragmentadas socavan directamente la eficacia de los técnicos y la productividad de las empresas.

Por qué el MTCR mejora la eficacia de los técnicos

Los procesos de recuperación limpia y libre de malware reducen la carga de trabajo de los técnicos:

- ✓ Se evitan los ciclos de reinfección.
- ✓ Se evita la necesidad de repetir las restauraciones.
- ✓ Se pierde menos tiempo cambiando constantemente entre herramientas.
- ✓ Se investigan y clasifican incidentes en menos tiempo.
- ✓ Se recupera la estabilidad operativa con mayor rapidez.
- ✓ Se gestionan más endpoints por técnico.

Reducir el MTCR multiplica el rendimiento de los técnicos en todos los clientes y entornos.



Cómo una plataforma unificada reduce el MTCR y el MTD

Funciones que reducen el tiempo de recuperación y las interrupciones:



Protección contra el ransomware asistida por IA



Validación de copias de seguridad impulsada por IA



Pruebas de recuperación aisladas



Flujos integrados de protección, detección y recuperación

Una arquitectura unificada acelera los procesos de recuperación limpia y reduce el tiempo de inactividad del negocio.

La ciberresiliencia no se trata solo de protección

Recuperación más limpia → Menos trabajo repetido

Menor tiempo de inactividad → Mayor productividad

Operaciones unificadas → MTCR más rápido

Mejor continuidad → Mejores resultados para los clientes

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.



[Más información](#)

[Contáctenos](#)