Información sobre ciberresiliencia

Brechas de ciberresiliencia, amenazas en evolución, defensas basadas en IA y estrategias de recuperación, en APJ en detalle

Los desafíos de ciberresiliencia se han intensificado a medida que los ciberataques y las carencias en la protección de datos aumentan los riesgos de interrupción. Las organizaciones con estrategias de ciberresiliencia maduras* tienen casi tres veces más probabilidades de recuperarse con éxito. Al modernizar las estrategias de resiliencia, mejorar las capacidades de detección y priorizar la optimización continua, los líderes de TI pueden minimizar los riesgos y reforzar la confianza en su capacidad para adaptarse a las amenazas en evolución.

Exceso de confianza en el liderazgo

El 74 % de los profesionales de TI opina que su liderazgo sobreestima el grado de preparación para cibereventos. Cuando un exceso de confianza toma el control, se generan puntos ciegos peligrosos que retrasan inversiones críticas y dejan vulnerabilidades sin atender.

La brecha entre confianza y capacidad

99,3 % de las organizaciones cuentan con estrategias de ciberseguridad

Sin embargo, **55 %** no logró recuperarse de manera efectiva de su última prueba o incidente

Prevención frente a recuperación: Un enfoque desequilibrado

87 % creen que su organización se centra más en prevenir los ataques que en prepararse para recuperarse de ellos

Y, aun así, solo **30 %** cuenta con una plataforma integral para la detección de amenazas en el almacenamiento primario, el almacenamiento de copia de seguridad y la infraestructura de red

Y solo **41 %** contuvo y se recuperó con éxito de un ataque o simulacro de incidente cibernético con un impacto mínimo

Es decir, cuando se producen las inevitables vulneraciones, muchas organizaciones no están preparadas para la fase de recuperación que determina la supervivencia empresarial.

El camino a seguir:
Las organizaciones maduras ofrecen resultados

Las organizaciones con estrategias de ciberresiliencia maduras son 2,8 veces más propensas a recuperarse con éxito

La madurez estratégica en estos tres pilares esenciales actúa de manera conjunta para crear una resiliencia inquebrantable.

GARANTIZAR LA SEGURIDAD:
Cree una base de confianza

Las organizaciones con estrategias de ciberresiliencia maduras son:

- **1,8 veces** más propensas a proteger los dispositivos mediante controles de seguridad a nivel de firmware o BIOS
- **Es más probable** aprovechar el cifrado para los datos en reposo y en tránsito
- **Es más probable** utilizar cibervaults para proteger los datos críticos frente a amenazas en evolución

Pero la seguridad solo es el principio. La verdadera ventaja procede de la detección inteligente que descubre las amenazas antes de que pongan en peligro sus activos más valiosos.

DETECTAR:
La inteligencia que nunca duerme

El reto de la visibilidad:
Solo el 30 % de las organizaciones cuentan con un sistema de detección de amenazas sólido en el almacenamiento de copias de seguridad, el almacenamiento de datos primario y la infraestructura de red

La solución con IA:

- **57 %** prioriza la inversión en detección de amenazas con tecnología de IA/ML
- **52 %** analiza exhaustivamente los datos de copia de seguridad con IA/ML para detectar indicadores de riesgo
- Las organizaciones con estrategias de resiliencia maduras son **2,3 veces más propensas** a usar herramientas de IA/aprendizaje automático con cuadernos de estrategias de mitigación y respuesta proactiva

RECUPERAR:
La preparación y el rendimiento, unidos

La ventaja de las pruebas:

- **61%** de las organizaciones que realizan simulaciones de ciberataques mensuales o con más frecuencia se recuperaron correctamente de incidentes
- **59 %** de las organizaciones que realizan menos de una prueba mensual no se recuperaron correctamente de los incidentes

El resultado:
Las organizaciones que realizan pruebas con frecuencia tienen una probabilidad significativamente mayor de cumplir tanto los objetivos de tiempo de recuperación como los objetivos de punto de recuperación, en comparación con las que realizan pruebas de manera esporádica.

Su camino hacia la excelencia en ciberresiliencia

Las organizaciones con estrategias de ciberresiliencia maduras son 2,3 veces más propensas a cumplir sus SLA de forma constante

Cree una base sólida
Priorice la prevención y la recuperación rápida.

- **Garantizar la seguridad:** Reduzca el riesgo con controles de seguridad a nivel del BIOS, cifrado de datos y cibervaults para datos críticos.
- **Detectar:** Utilice IA/aprendizaje automático en tiempo real para detectar y responder a amenazas en todo el almacenamiento, es decir, el almacenamiento primario y el de protección.
- **Recuperar:** Pruebe la recuperación con frecuencia: las organizaciones que lo hacen mensualmente tienen muchas más probabilidades de cumplir sus objetivos de recuperación.

¿Todo listo para mejorar la ciberresiliencia?

¿Todo listo para mejorar la ciberresiliencia? Lea todos los datos clave de la *investigación sobre ciberresiliencia de Dell 2026.*

DELL Technologies

Fuente: Encuesta sobre ciberresiliencia realizada por Vanson Bourne y Dell Technologies, 2025.

* Se consideran organizaciones con estrategias de ciberresiliencia maduras aquellas que cuentan con una estrategia plenamente establecida y en continua optimización, basada en análisis predictivo, automatización y conocimientos en tiempo real (por ejemplo, fuentes de Threat intelligence, ajustes por aprendizaje automático y KPI personalizados para la mejora).