Ciberresiliencia en acción

Evaluación comparativa de la preparación empresarial global en seguridad, detección y recuperación
Debate sobre la información
Enero de 2026.

DELL Technologies

Programa

- Objetivos y firmografías
- La brecha de ciberresiliencia
- Seguridad
- Detección
- Recuperación
- Complejidad, cultura y futuro

Objetivos empresariales

- Posicionar a Dell como líder de opinión y socio estratégico para la ciberresiliencia
- Reafirmar la decisión de cambiar el enfoque de "protección de datos" a "resiliencia cibernética"

Objetivos de la investigación

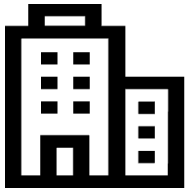
- Evaluar la madurez y la integración de las estrategias de ciberresiliencia
- Evaluar la eficacia de las prácticas de seguridad, detección y recuperación de las organizaciones
- Conocer las barreras que impiden mejorar la ciberresiliencia, lo que incluye las carencias de conocimientos, el presupuesto y la complejidad
- Explorar cómo las organizaciones protegen su entorno de TI y los datos frente a las amenazas de ransomware

¿A quién entrevistamos?

Se entrevistó a los encuestados en julio y octubre de 2025

850 responsables de la toma de decisiones de TI de organizaciones globales

Organizaciones con más de 1000 empleados



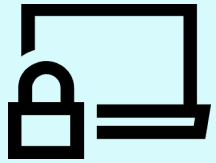
Organizaciones de una gran variedad de sectores públicos y privados

Los encuestados son: Miembros de la junta directiva y gerentes superiores de nivel intermedio

Resultados clave

39 %

de las organizaciones cuentan con una estrategia de ciberresiliencia totalmente establecida y optimizada continuamente



La optimización continua es clave: sin ella, las estrategias pueden quedar obsoletas rápidamente frente a las amenazas en constante evolución, lo que provoca que las organizaciones corran un mayor riesgo

46 %

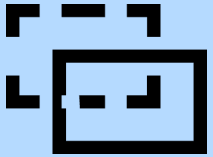
reconocen que sus datos de copia de seguridad no están tan protegidos como deberían

Reforzar la protección de las copias de seguridad es esencial para garantizar que la recuperación siga siendo posible cuando los sistemas primarios se vean comprometidos.

Seguridad

30 %

utilizan una plataforma completa para la detección de amenazas en la red, las copias de seguridad y el almacenamiento principal



Sin una detección unificada, la visibilidad de las amenazas y los tiempos de respuesta pueden ser más lentos, lo que aumenta el riesgo de vulneraciones no detectadas.

Detección

55 %

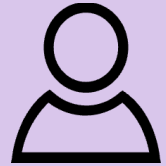
de los que realizaron ciberataques simulados mensualmente o con mayor frecuencia se recuperaron con éxito de un incidente cibernético o de perforación

Las pruebas frecuentes ayudan a los equipos a prepararse para la situación real. Los equipos que no están preparados corren el riesgo de retrasar la respuesta y la recuperación cuando más se necesitan.

Recuperación

63 %

creen que los responsables sobreestiman la preparación de su organización para un ciberevento importante



El exceso de confianza puede detener las inversiones, retrasar la planificación de la respuesta y dejar sin abordar las vulnerabilidades críticas.

DELL Technologies

Sección 1: La brecha de ciberresiliencia

Comprender el problema y la urgencia de evolucionar

La optimización continua de las estrategias de resiliencia mejora la recuperación, pero el éxito no está garantizado

99,5 %

tienen una estrategia de ciberresiliencia de algún tipo

39 %

creen que está totalmente establecida y optimizada continuamente (una estrategia madura)

57 %

no contuvieron ni se recuperaban de forma eficaz durante la última prueba o incidente

Las organizaciones con estrategias de ciberresiliencia maduras tienen **2,6 veces más probabilidades de recuperarse** con éxito

65 % frente a. **25 %**

63 %

creen que los **responsables sobreestiman su preparación** para un ciberevento importante

Por qué esto importa ahora

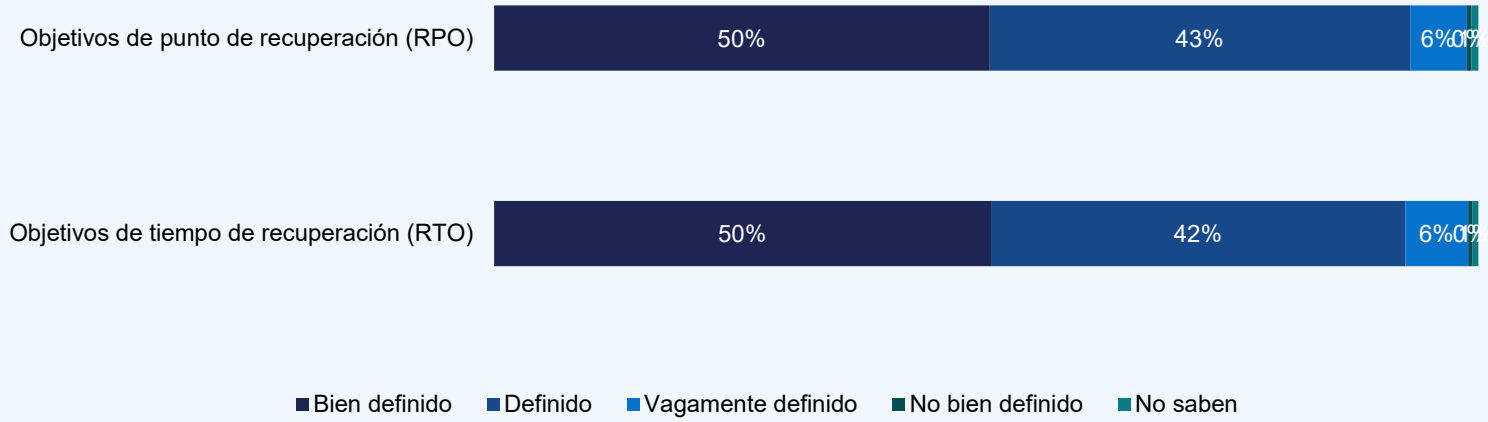
97 %

están de acuerdo en que su organización debe reforzar continuamente la seguridad a medida que evolucionan las amenazas

78 %

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

La extensión que han definido las organizaciones:



32 %

Tienen **ambas áreas** bien definidas

De aquellos con una estrategia de ciberresiliencia madura

58 %

Tienen tanto los RTO como los RPO bien definidos

Sección 2: Seguridad

Prevención de ataques y refuerzo del entorno digital

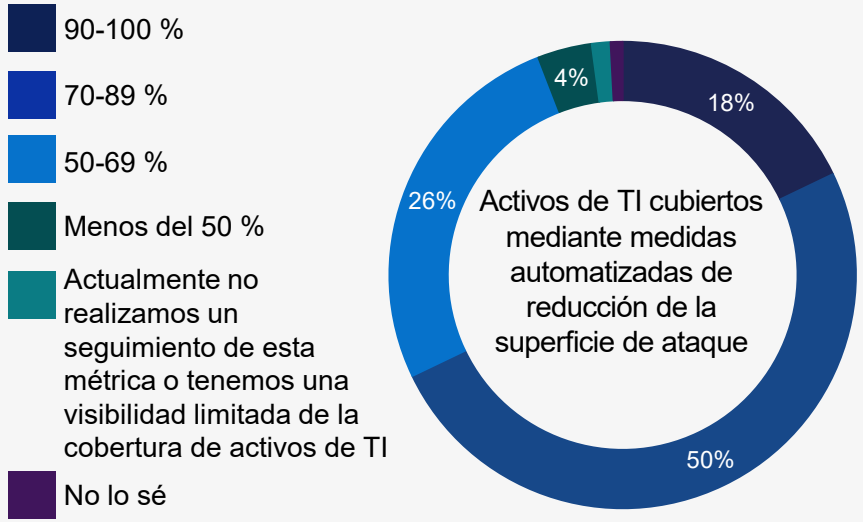
Carencias de visibilidad y protección

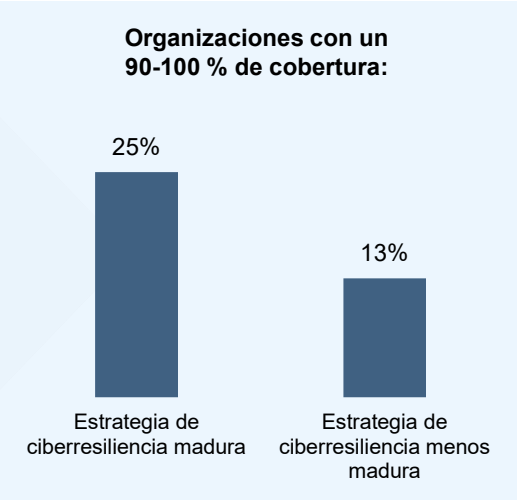
46 %

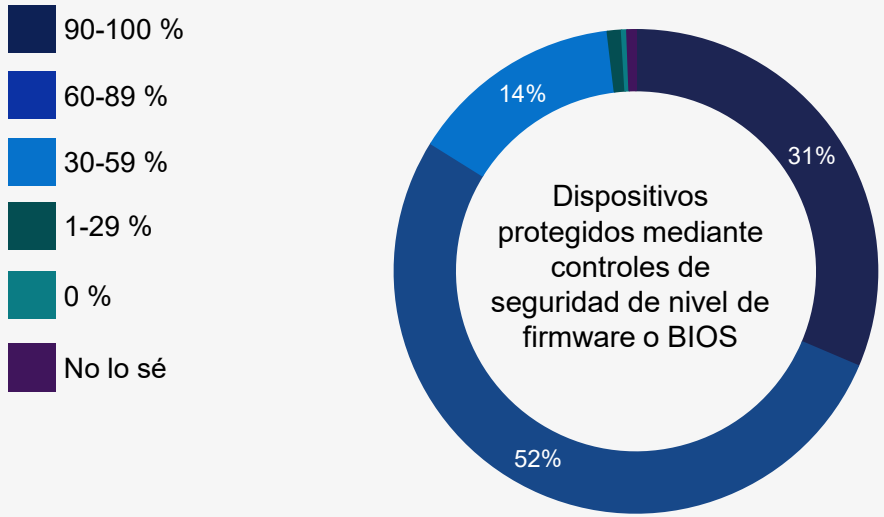
admiten que sus datos de copia de seguridad no están tan protegidos como deberían

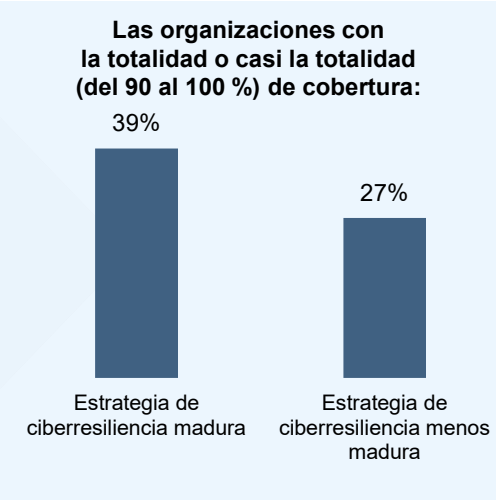
N/A	**59 %**
EMEA	**43 %**
LATAM	**41 %**
APJ	**39 %**

La optimización continua no elimina las carencias de cobertura, pero proporciona a las organizaciones una ventaja crítica en resiliencia









Desde la integridad previa a la implementación hasta la recuperación posterior al ataque: refuerce ambos extremos de la seguridad

Procesos y métodos utilizados por las organizaciones para garantizar la integridad del hardware y el software de TI

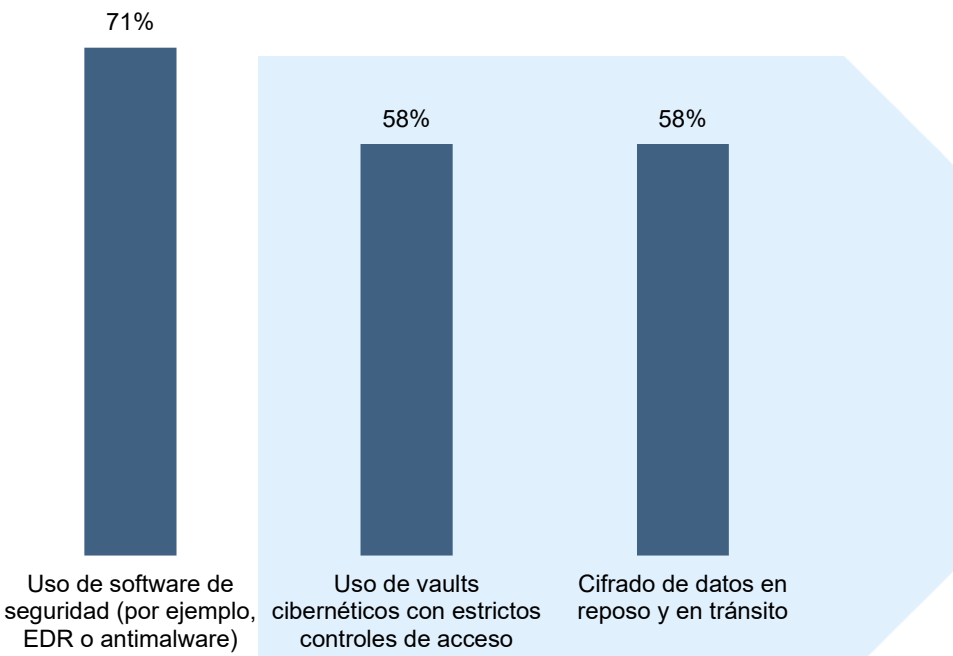
72 %

confían en los proveedores para obtener certificaciones y acreditaciones, así como sistemas con herramientas integradas que verifican la integridad de los componentes

64 %

realizan auditorías internas o revisiones manuales durante la preparación o la implementación

Métodos utilizados por las organizaciones para proteger los datos críticos frente a ataques de ransomware



Las organizaciones con estrategias de resiliencia maduras son más propensas a utilizar:

- **Cifrado de datos (59 % frente a 57 %)**
- **Cyber Vault (63 % frente a 55 %)**

que las organizaciones con estrategias de resiliencia menos maduras

Sección 3: Detección

Detectar amenazas y responder a ellas antes de que se produzca un impacto

El uso de la IA y la automatización permitiría detectar las amenazas antes de que pongan en peligro las copias de seguridad

38 %

de las organizaciones utilizan herramientas de IA/ML con cuadernos de estrategias de respuesta y mitigación proactivas

Las organizaciones con una estrategia de ciberresiliencia madura son **3,1 veces más** propensas a hacer esto

65 % frente a. **21 %**

48 %

de las organizaciones utilizan **IA/ML ampliamente para analizar los datos de copia de seguridad** en busca de indicadores de riesgo

El uso extensivo de IA/ML se produce **2,3 veces más a menudo en organizaciones con una estrategia de ciberresiliencia madura**

72 % frente a. **32 %**

83 %

creen que los atacantes **atacan cada vez más las copias de seguridad** durante los ataques de ransomware

62 % priorizan la inversión en automatización y detección de amenazas con tecnología de IA/ML

La visibilidad incompleta aumenta el riesgo

54 %

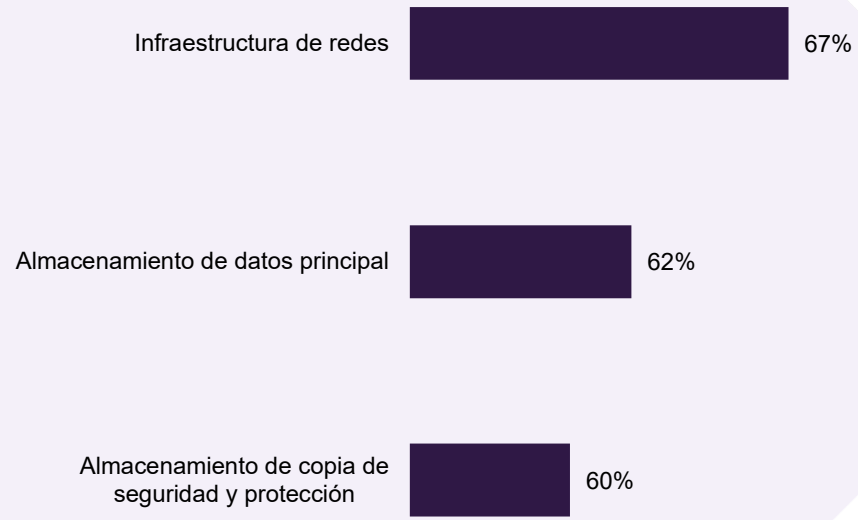
afirman que tienen una alta visibilidad de la actividad sospechosa o los datos en riesgo dentro de sus sistemas de copia de seguridad

74 % de organizaciones con una estrategia de ciberresiliencia madura

frente a

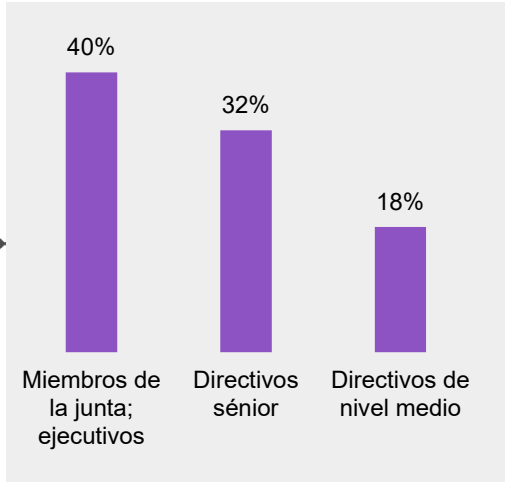
42 % de organizaciones con una estrategia de ciberresiliencia menos madura

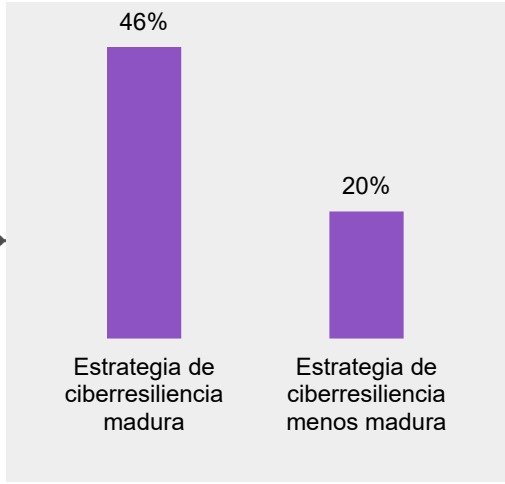
Organizaciones con una plataforma sólida para la detección de amenazas en las siguientes áreas



30 %

tienen una plataforma completa **en las 3 áreas**





Sección 4: Recuperación

Recuperarse rápidamente y dentro de las expectativas del SLA

Estado de la recuperación: muchas organizaciones cumplen los objetivos, pero es esencial una mejora continua para mantenerse al día con el panorama de amenazas

40 %

de las organizaciones **resistieron y se recuperaron adecuadamente** con el mínimo impacto

Los **miembros de la junta directiva (53 %)** son más propensos a afirmarlo que los **directivos de nivel medio (30 %)**

54 %

de las organizaciones alcanzaron sus **objetivos de RTO/RPO**

Por puesto: miembros de la junta directiva (45 %) frente a directivos de nivel medio (66 %)

N.º 4

El principal impulsor de la inversión en ciberseguridad es un **ciberincidente o cuasi incidente reciente** en nuestra organización

57 % están mejorando las capacidades de resiliencia para **cumplir con requisitos normativos o de cumplimiento**

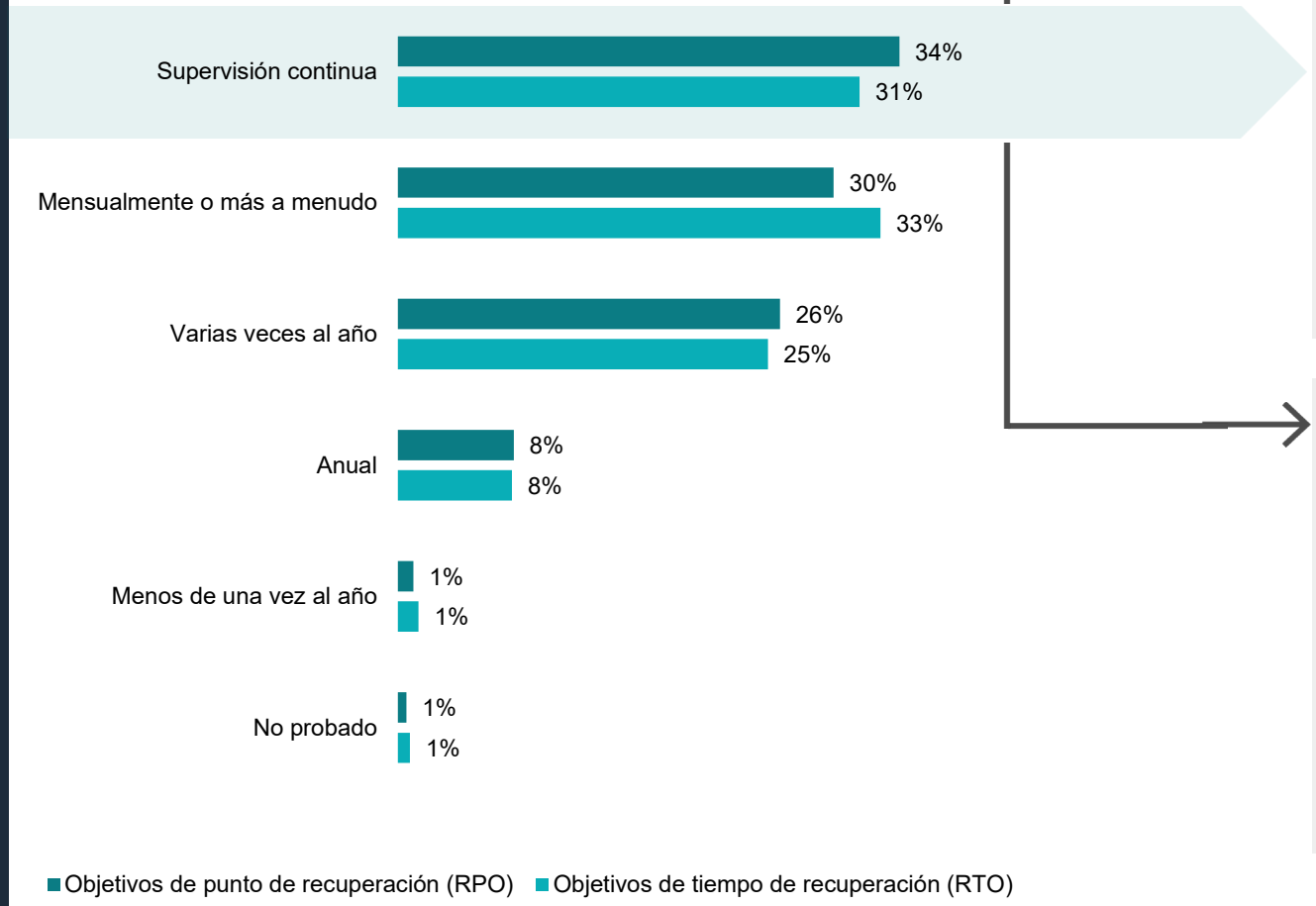
Las pruebas frecuentes podrían mejorar la recuperación

En última instancia, una cultura de alerta y mejora constante es lo que genera resiliencia.

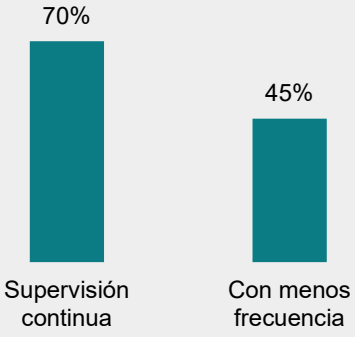
Directivo sénior, organización de servicios para consumidores, Brasil

Las pruebas son cruciales para la resiliencia, ya que ofrecen a las organizaciones una mejor oportunidad de recuperarse

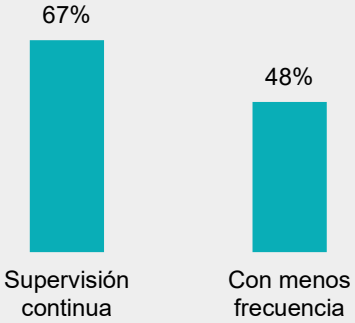
Frecuencia de las pruebas de RTO/RPO



Cumplimiento de los objetivos de RPO/RTO mediante pruebas: objetivos de punto de recuperación (RPO)



Cumplimiento de los objetivos de RPO/RTO mediante pruebas: objetivos de tiempo de recuperación (RTO)



Las pruebas son fundamentales para la resiliencia

48 %

afirmaron que las pruebas de ciberseguridad de su organización no simulan de manera realista las técnicas de ataque modernas

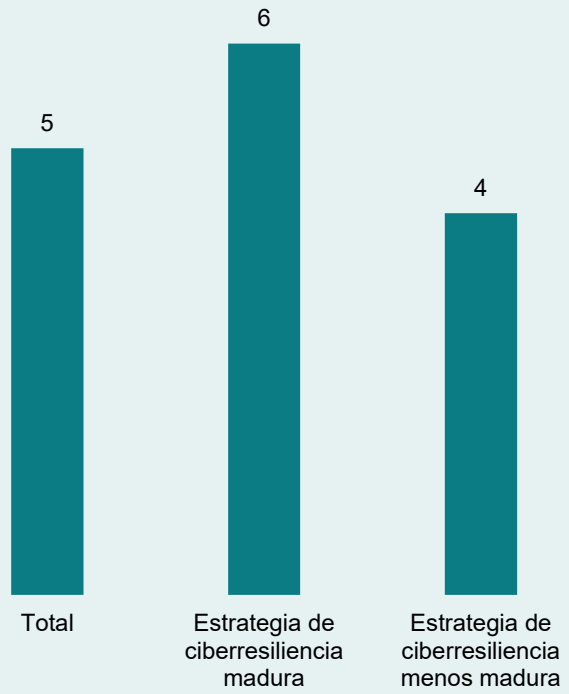
53 % de los miembros de la junta; ejecutivos

frente a

48 % de los directivos de nivel medio

La práctica regular es clave para mejorar la recuperación, pero las organizaciones deben planificar continuamente para las amenazas en evolución

Media de veces al año que las organizaciones realizan ciberataques simulados



55 %

de los que realizaron ciberataques simulados **mensualmente o con mayor frecuencia se recuperaron con éxito** de un incidente cibernético o de perforación

35 %

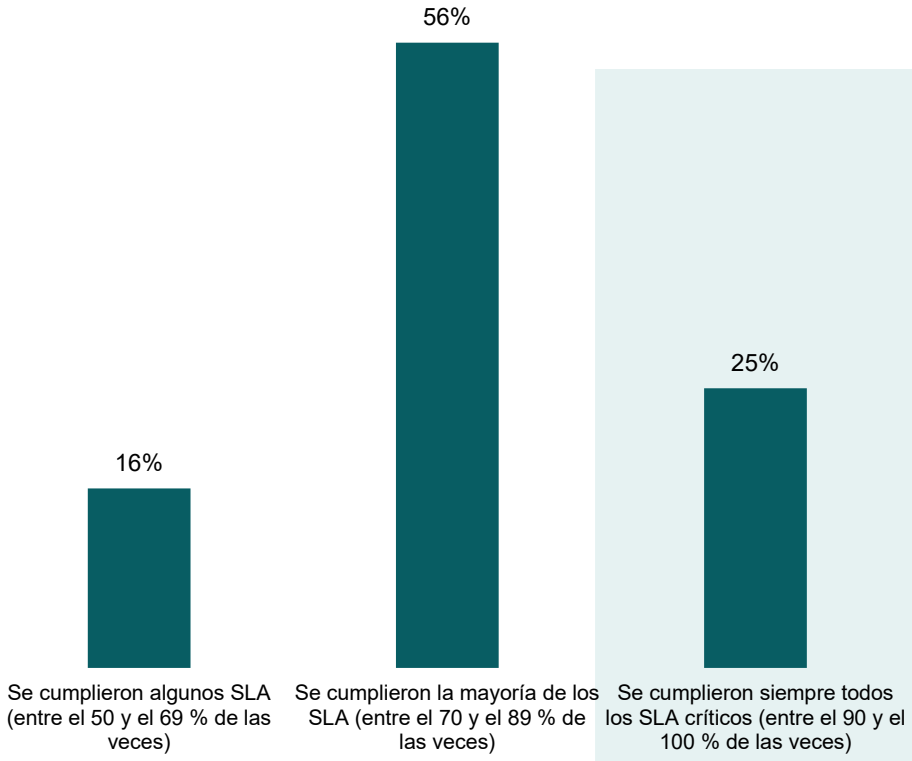
de los que realizaron ciberataques simulados **menos de una vez al mes se recuperaron con éxito de** un incidente cibernético o de perforación

> *La necesidad de probar y evaluar de forma integral todas las superficies de amenazas potenciales en lugar de centrarse en la cobertura y las pruebas puntuales.*
>
> Directivo sénior, tecnología de TI y telecomunicaciones, Reino Unido

> *Los ciberataques nos recuerdan lo importante que es realizar simulacros de seguridad periódicos.*
>
> *Se ha reforzado la formación en concienciación sobre seguridad, lo que permite a todos los empleados identificar posibles amenazas.*
>
> Miembro de la junta, construcción y propiedades, Australia

Los SLA son el punto de prueba: las organizaciones con estrategias maduras cumplen sus promesas de recuperación

Frecuencia de las organizaciones que cumplen los SLA para la recuperación crítica del sistema

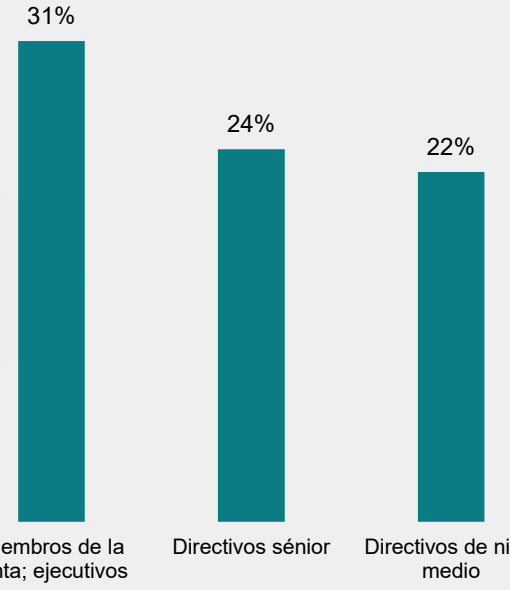


El doble

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

36 % frente a. **18 %**

Por puesto:



Sección 5: Complejidad, cultura y futuro

Barreras organizativas y planes de inversión futuros

La complejidad, las carencias de habilidades y el exceso de confianza amenazan la ciberresiliencia, pero la IA y la formación podrían ayudar

Principales retos:

Entornos de TI complejos	49 %
Limitaciones presupuestarias	42 %
Falta de personal cualificado	39 %
Fragmentación de proveedores/ herramientas	38 %
Baja priorización de los ejecutivos	23 %

Las organizaciones más grandes tienen más probabilidades de enfrentarse a esto:

50 % A partir de 5000 empleados

50 % 3000-4999 empleados

46 % 1000-2999 empleados

63 %

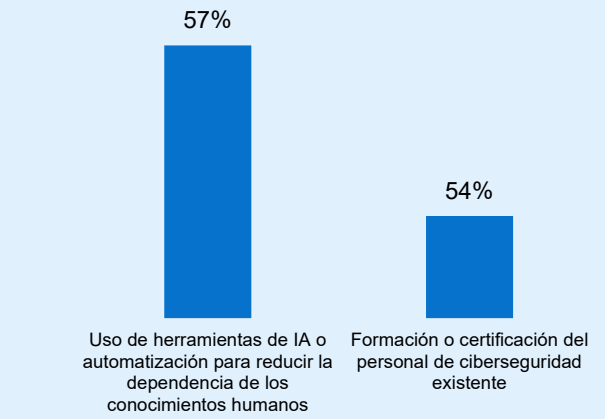
creen que los responsables sobreestiman la preparación de su organización para un ciberevento importante

96 %

reconocen que tienen deficiencias en sus habilidades o conocimientos sobre ciberseguridad

PERO…

Las organizaciones actúan a través de:



De cara al futuro de las inversiones

N.º 1

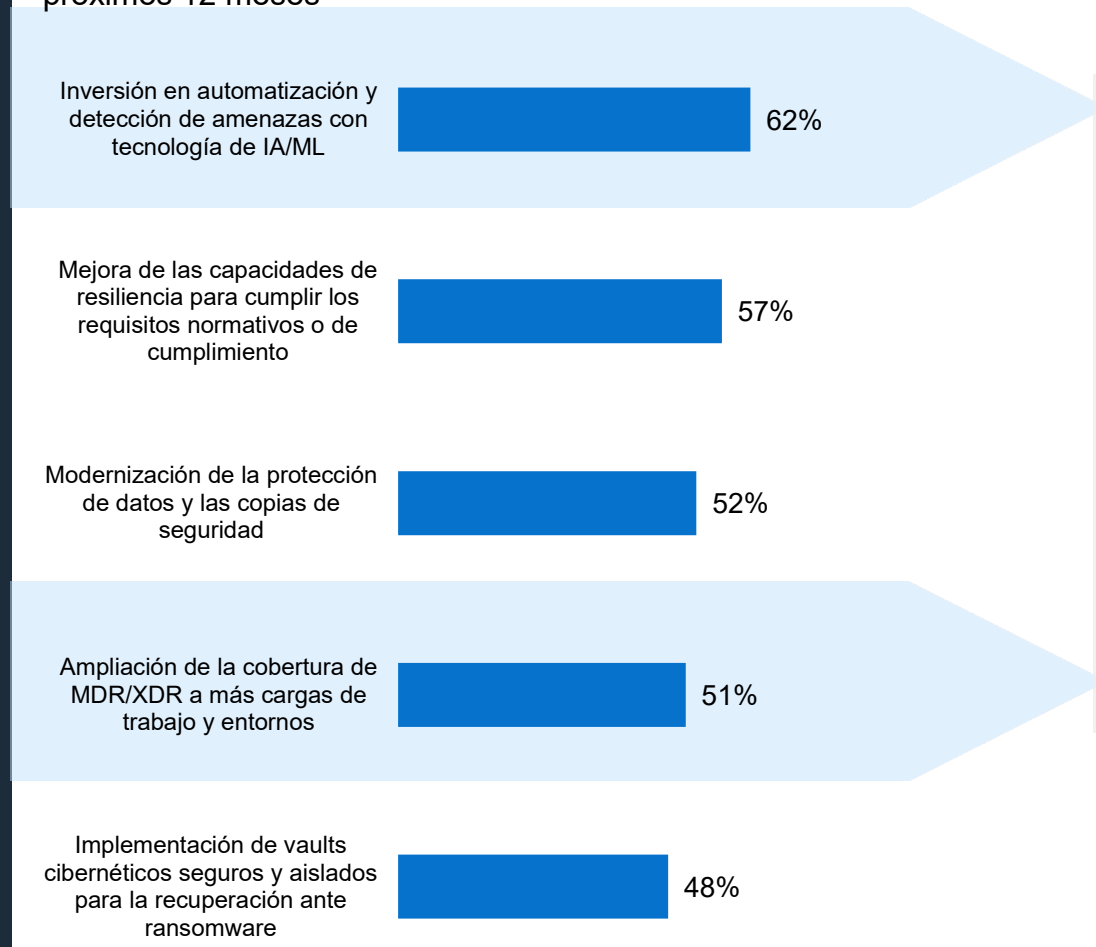
El motor de la inversión es el panorama de amenazas en evolución

97 %

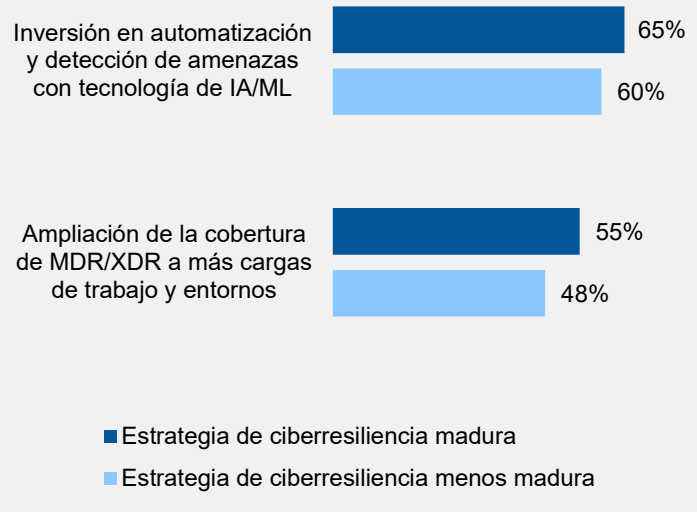
"Mi organización debe reforzar continuamente su seguridad a medida que evolucionan las amenazas"

Para mantener una postura madura, la inversión y la optimización continuas son el camino a seguir

Inversiones en ciberresiliencia priorizadas en los próximos 12 meses



Las organizaciones ciberresilientes maduras invierten continuamente

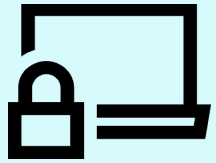


Nociones clave

Resultados clave

39 %

de las organizaciones cuentan con una estrategia de ciberresiliencia totalmente establecida y optimizada continuamente



La optimización continua es clave: sin ella, las estrategias pueden quedar obsoletas rápidamente frente a las amenazas en constante evolución, lo que provoca que las organizaciones corran un mayor riesgo

46 %

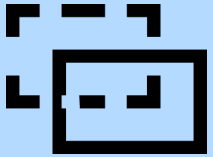
reconocen que sus datos de copia de seguridad no están tan protegidos como deberían

Reforzar la protección de las copias de seguridad es esencial para garantizar que la recuperación siga siendo posible cuando los sistemas primarios se vean comprometidos.

Seguridad

30 %

utilizan una plataforma completa para la detección de amenazas en la red, las copias de seguridad y el almacenamiento principal



Sin una detección unificada, la visibilidad de las amenazas y los tiempos de respuesta pueden ser más lentos, lo que aumenta el riesgo de vulneraciones no detectadas.

Detección

55 %

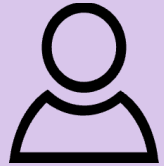
de los que realizaron ciberataques simulados mensualmente o con mayor frecuencia se recuperaron con éxito de un incidente cibernético o de perforación

Las pruebas frecuentes ayudan a los equipos a prepararse para la situación real. Los equipos que no están preparados corren el riesgo de retrasar la respuesta y la recuperación cuando más se necesitan.

Recuperación

63 %

creen que los responsables sobreestiman la preparación de su organización para un ciberevento importante



El exceso de confianza puede detener las inversiones, retrasar la planificación de la respuesta y dejar sin abordar las vulnerabilidades críticas.

DELL Technologies

DELL Technologies