Ciber Resiliencia en acción

¿Cómo están preparadas las organizaciones de Latinoamérica en Seguridad, Detección y Recuperación?

Enero de 2026

DELL Technologies

Agenda

- Objetivos
- La brecha de la ciberresiliencia
- Seguridad
- Detección
- Recuperación
- Complejidad, cultura y lo que viene

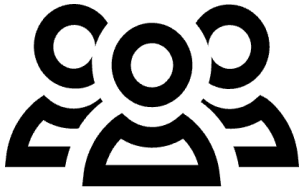
Objetivos de la investigación

- Evaluar la madurez e integración de las estrategias de ciberresiliencia
- Evaluar la eficacia de las organizaciones en las prácticas de seguridad, detección y recuperación
- Comprender las barreras para mejorar la ciberresiliencia, incluyendo las carencias de habilidades, el presupuesto y la complejidad
- Explorar cómo las organizaciones están protegiendo su entorno informático y protegiendo los datos de amenazas de ransomware

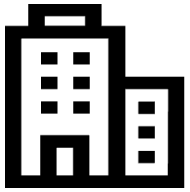
¿A quién entrevistamos?

Los encuestados fueron entrevistados en octubre de 2025

100 responsables de la toma de decisiones de TI de organizaciones en LATAM



Organizaciones con +1.000 empleados



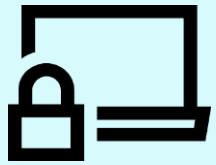
Organizaciones de diversas industrias públicas y privadas

Los encuestados son:
Miembros de la junta; Nivel C
Directivos superiores
Directivos de nivel medio

Hallazgos clave

36%

de las organizaciones cuentan con una estrategia de ciberresiliencia completamente establecida y optimizada de forma continua



La optimización continua es clave: sin ella, las estrategias pueden quedar rápidamente obsoletas frente a amenazas en evolución, dejando a las organizaciones en mayor riesgo

41%

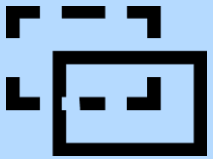
reconocer que sus datos de copia de seguridad no están tan bien protegidos como deberían

Reforzar la protección de respaldo es esencial para garantizar que la recuperación siga siendo posible cuando los sistemas principales se vean comprometidos.

Secure

37%

Utiliza una plataforma integral para la detección de amenazas en red, copia de seguridad y almacenamiento primario



Sin una detección unificada, la visibilidad y los tiempos de respuesta de amenazas pueden ser más lentos, aumentando el riesgo de brechas no detectadas.

Detect

48%

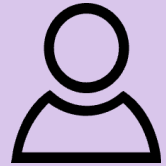
de quienes realizaron ciberataques simulados mensualmente o con más frecuencia se recuperaron con éxito de un simulacro o incidente cibernético

Las pruebas frecuentes ayudan a los equipos a prepararse para lo real. Los equipos que no están preparados arriesgan la respuesta y recuperación tardía cuando más importa.

Recover

56%

Piensa que la dirección sobreestima la preparación de su organización ante un gran evento cibernético



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

Sección 1: La brecha de resiliencia cibernética

Comprender el problema y la urgencia de evolucionar

Optimizar continuamente las estrategias de resiliencia mejora la recuperación, pero el éxito no está garantizado

100%

Tener una estrategia de ciberresiliencia de algún tipo

36%

Cree que está completamente establecido y continuamente optimizado (una estrategia madura)

59%

no se contuvieron ni recuperaron eficazmente durante su última prueba o incidente

Las organizaciones con estrategias maduras de ciberresiliencia tienen 2,3 veces más probabilidades de recuperarse con éxito

64% Vs. **28%**

56%

cree que el liderazgo sobreestima su preparación para un gran evento cibernético

Por qué esto importa ahora

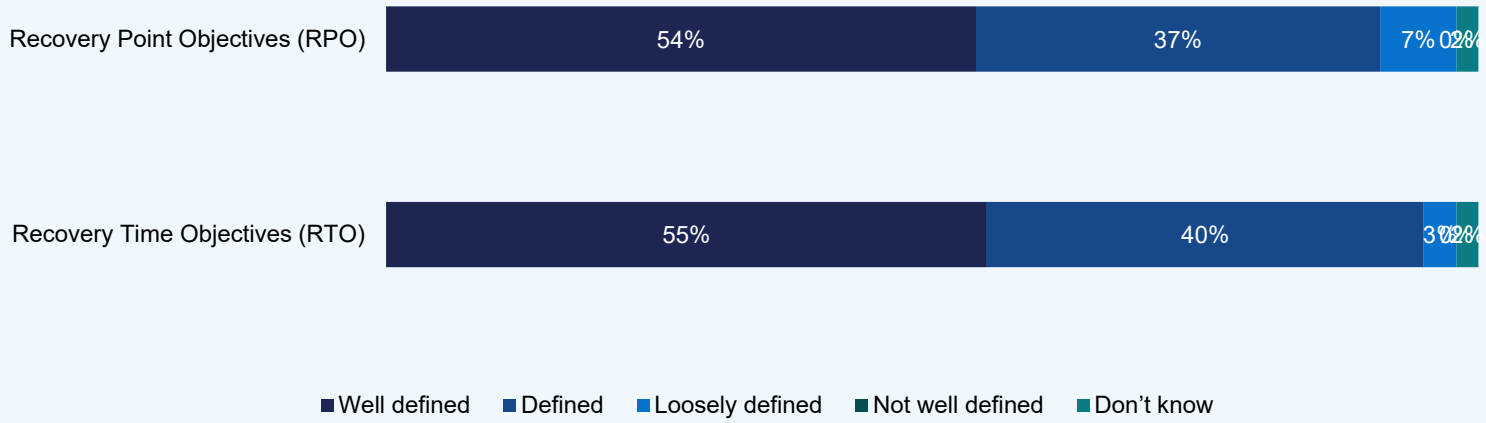
97%

Coincide en que su organización necesita reforzar continuamente la seguridad a medida que evolucionan las amenazas

66%

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

El alcance que las organizaciones han definido:



38%

Que ambas áreas estén bien definidas

De aquellos con una estrategia madura de ciberresiliencia

50%

Tienen tanto un RTO como un RPO bien definidos

Sección 2: Seguridad

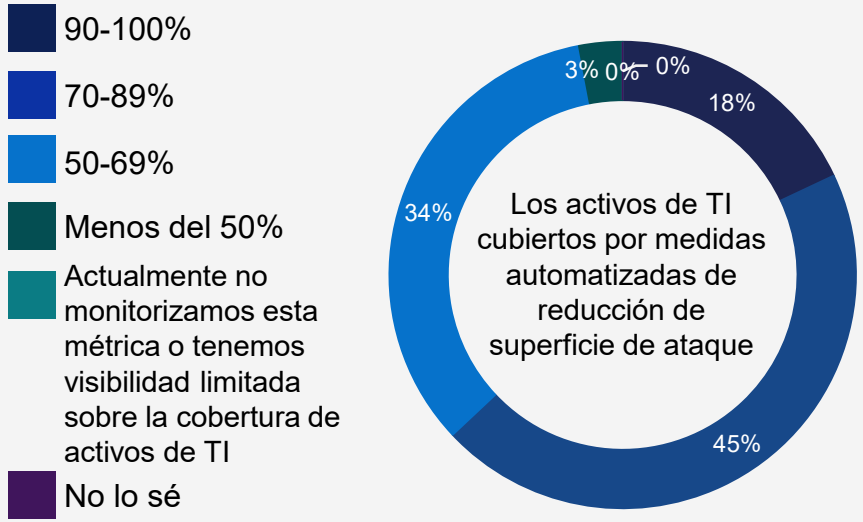
Prevención de ataques y fortalecimiento del patrimonio digital

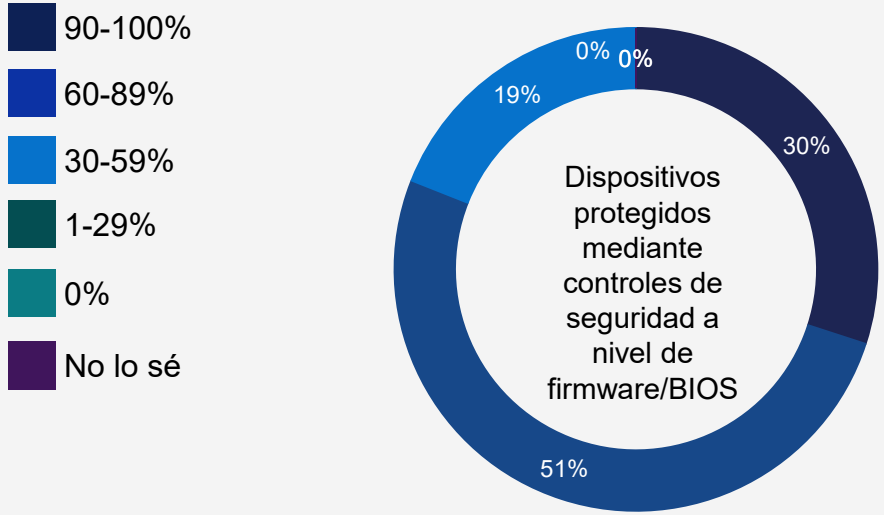
Brechas de visibilidad y deficiencias de protección

41%

admite que sus datos de respaldo no están tan bien protegidos como deberían

La optimización continua no elimina las lagunas de cobertura, pero sí otorga a las organizaciones una ventaja crítica en resiliencia





Desde la integridad previa al despliegue hasta la recuperación tras ataque: fortalecer ambos extremos de la seguridad

Procesos/Métodos utilizados por las organizaciones para garantizar la integridad del hardware/software de TI

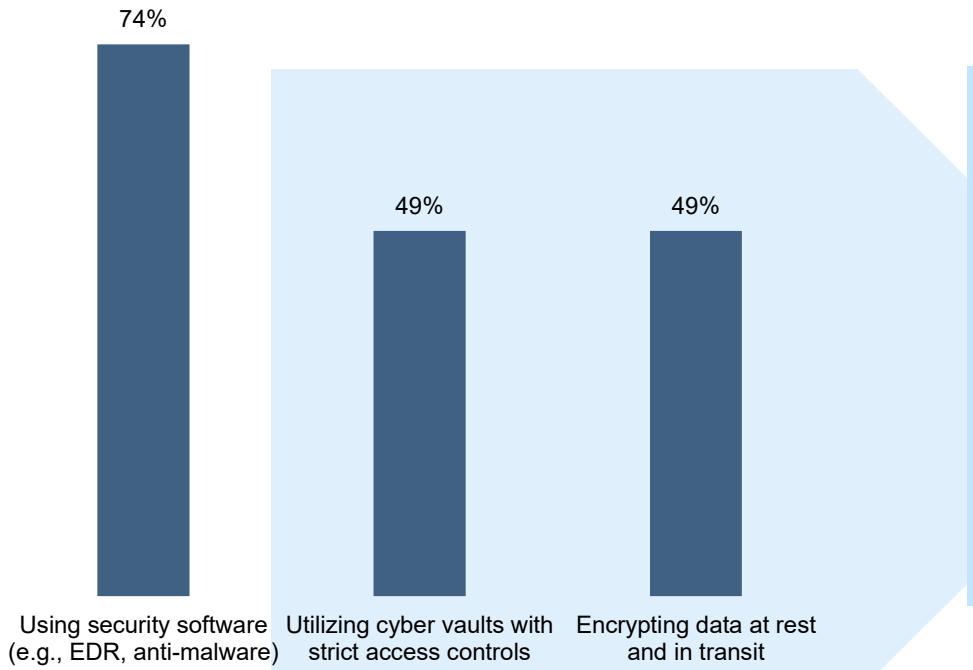
80%

Depende de los proveedores para certificaciones, así como de sistemas con herramientas integradas que verifiquen la integridad de los componentes

67%

Realiza auditorías internas o revisiones manuales durante la preparación/despliegue

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



Organizaciones con estrategias de resiliencia maduras más propensas a utilizar:
Ciber Bóvedas
(64%vs 41%)

que organizaciones con estrategias de resiliencia menos maduras

Sección 3: Detección

Detectar y responder a amenazas antes del impacto

Utilizar IA y automatización podría descubrir amenazas antes de que comprometan las copias de seguridad

38%

de las organizaciones utilizan herramientas de IA/ML con manuales proactivos de mitigación y respuesta

Las organizaciones con una estrategia madura de ciberresiliencia tienen tres veces más probabilidades de hacerlo

67% Vs. **22%**

45%

de las organizaciones utilizan IA/ML extensamente para escanear datos de respaldo en busca de indicadores de compromiso

El uso extensivo de IA/ML ocurre 2,7 veces más en organizaciones con una estrategia madura de ciberresiliencia

75% Vs. **28%**

78%

Cree que los actores maliciosos atacan cada vez más copias de seguridad durante ataques de ransomware

están priorizando invertir en automatización y detección de amenazas impulsada por IA/ML

68%

La visibilidad incompleta aumenta el riesgo

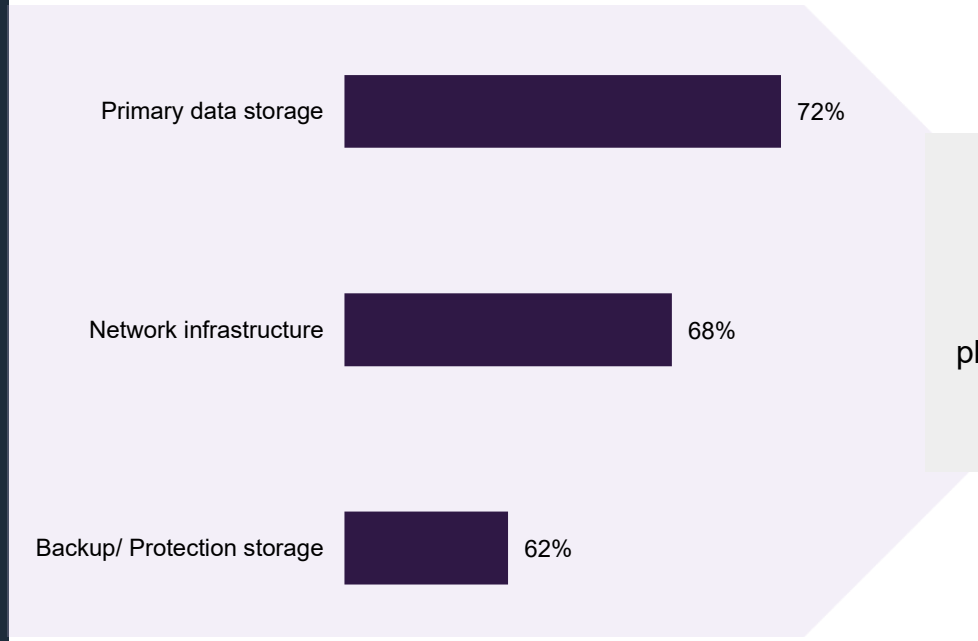
55%
Dicen tener alta visibilidad sobre actividades sospechosas o datos comprometidos dentro de sus sistemas de respaldo

92% Organizaciones con una estrategia madura de ciberresiliencia

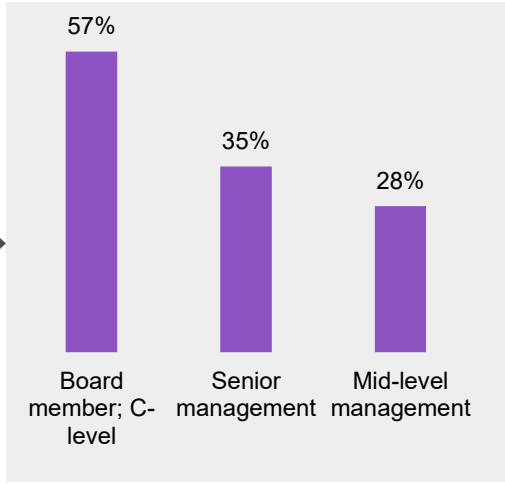
Vs

34% de organizaciones con una estrategia de ciberresiliencia menos madura

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



37%
Tiene una plataforma completa en las tres áreas



Sección 4: Recuperación

Recuperándonos rápido y dentro de las expectativas del SLA

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

41%

contenida y recuperada con éxito con impacto mínimo

Con **miembros de la junta (43%) menos propensos** a afirmar esto que los **directivos de nivel medio (50%)**

58%

de organizaciones cumplieron sus objetivos de RTO/RPO

Por puesto: Miembros de la Junta (50%) Vs Dirección de nivel medio (63%)

#3

El principal motor de la inversión en ciberseguridad es un incidente cibernético reciente o un casi accidente en la organización

56% está mejorando las capacidades de resiliencia para cumplir con los requisitos regulatorios o de cumplimiento

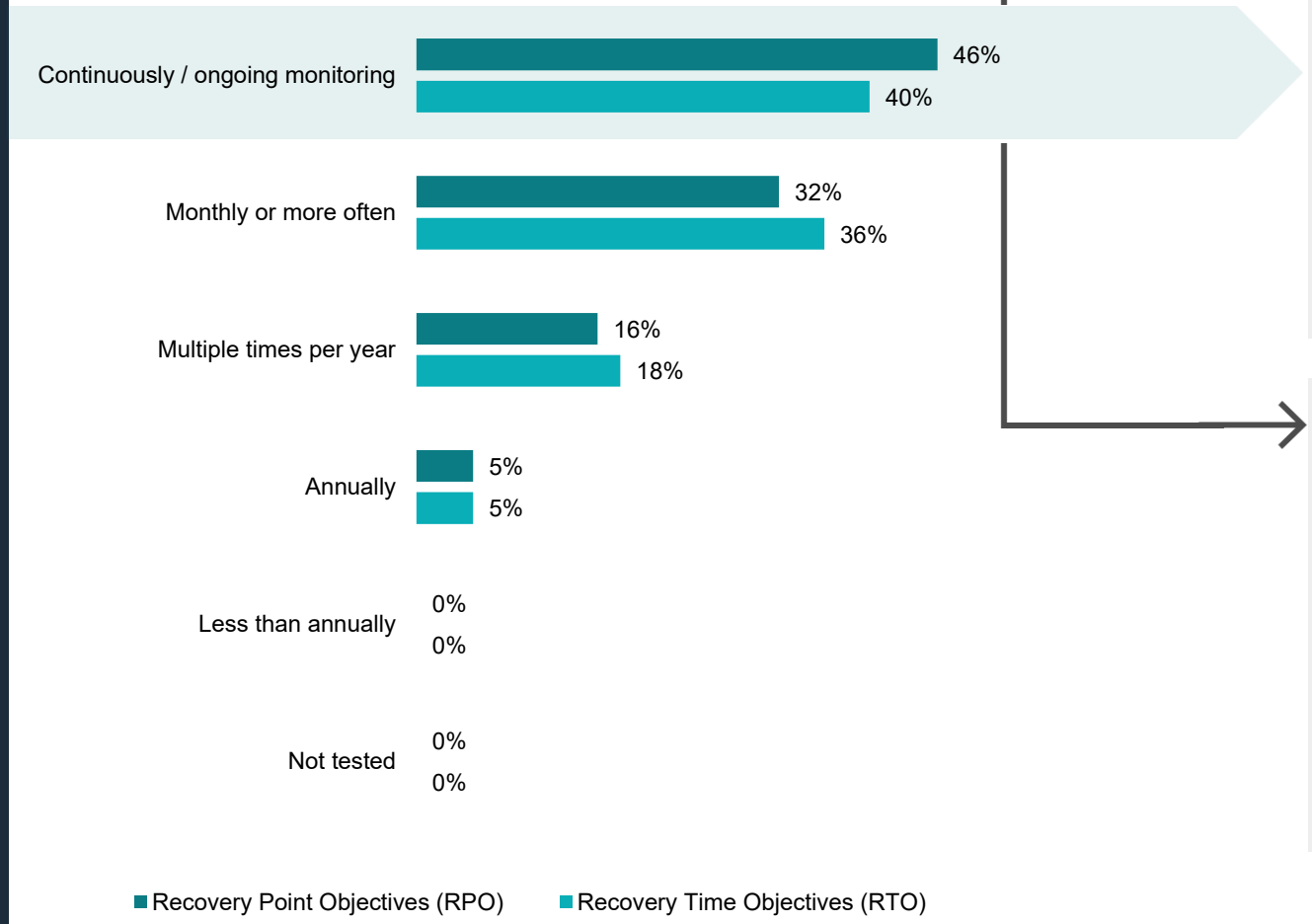
Realizar pruebas frecuentes podría mejorar la recuperación

Las evaluaciones regulares de vulnerabilidades ayudan a identificar debilidades antes de que los atacantes puedan explotarlas.

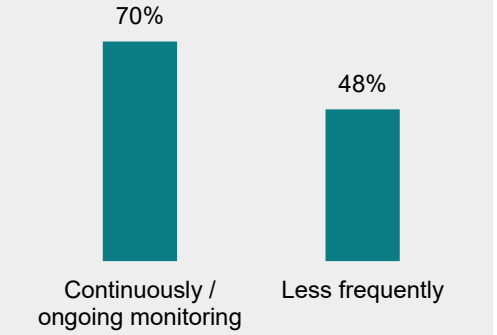
Gerente Senior de Sector Público, México

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

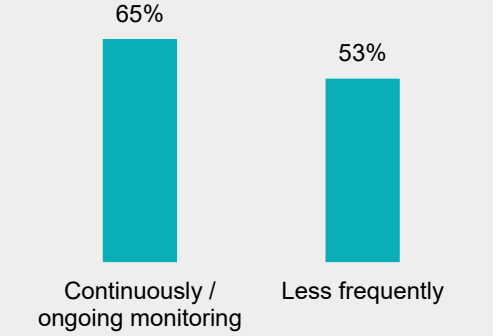
Frecuencia de pruebas RTO/RPO



Cumplimiento de los objetivos de RPO/RTO mediante pruebas: Objetivos de Puntos 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

44%

Afirma que las pruebas de ciberseguridad de su organización no simulan de forma realista las técnicas modernas de ataque

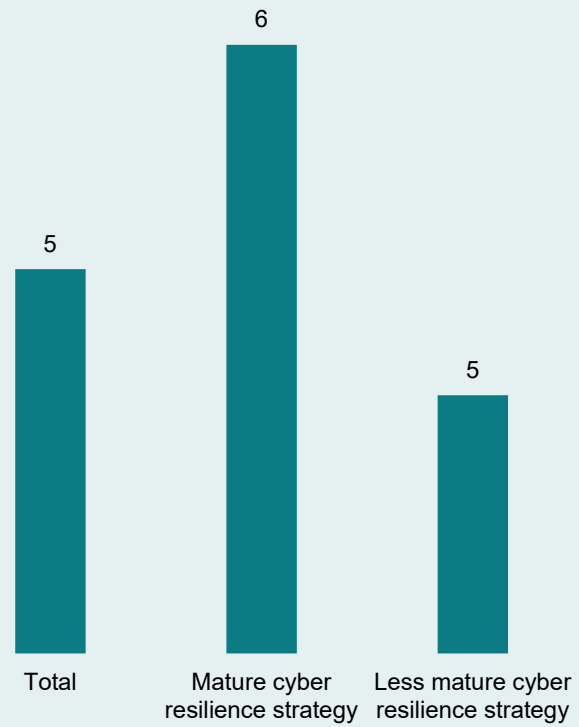
29% de miembros de la junta; C-Level

Vs

44% de la gestión de nivel medio

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

En promedio al año, las organizaciones realizan ciberataques simulados



Filtro: Región = LATAM

48%

de quienes realizaron ciberataques simulados mensualmente o con más frecuencia se recuperaron con éxito de un simulacro o incidente cibernético

38%

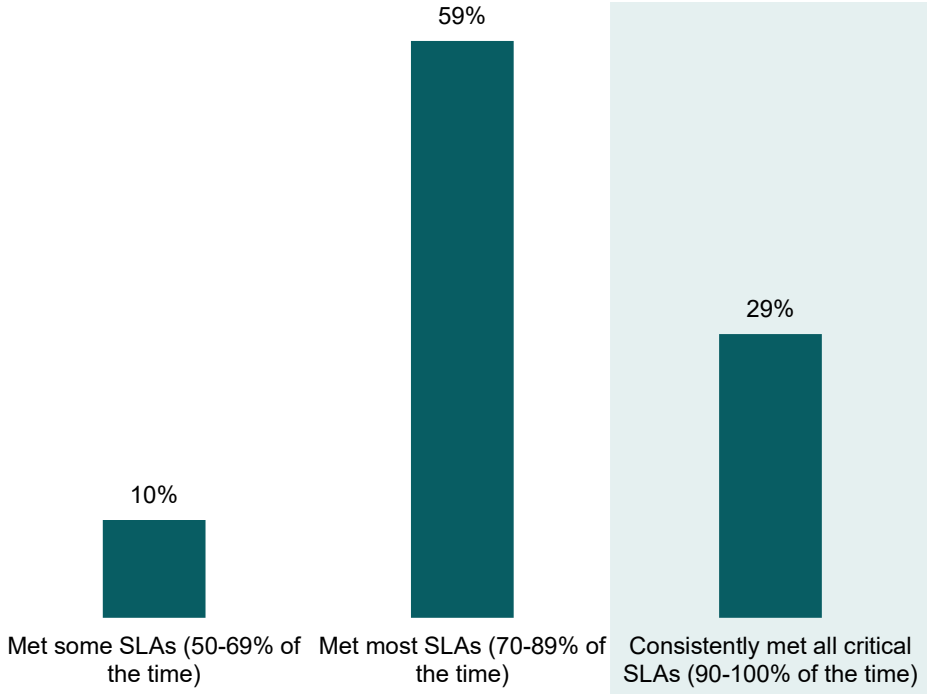
de aquellos que realizaron ciberataques simulados en menos de un mes se recuperaron con éxito de un simulacro/incidente cibernético

> *Debemos ser más conscientes de que las amenazas de ciberseguridad están evolucionando hoy a un ritmo mucho más acelerado, por lo que nuestros esfuerzos por modernizar nuestra seguridad también deben mantenerse al día.*
> Gerente Senior, Fabricación, México

> *No se trata de evitar los ciberataques, sino de asumir que inevitablemente ocurrirán.*
> Gerente Senior, IT/Tech, México

Los SLA son la prueba: las organizaciones con estrategias maduras cumplen las promesas de recuperación

Frecuencia con la que las organizaciones cumplen los SLAs para la recuperación crítica del sistema

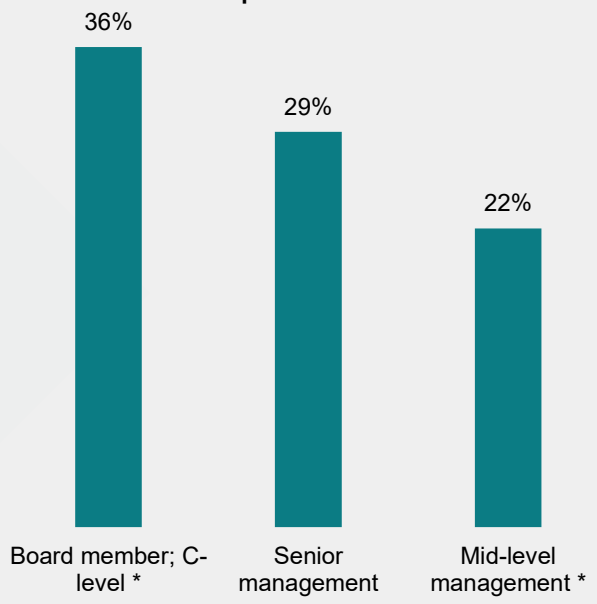


1.9x

Las organizaciones con estrategias maduras de ciberresiliencia tienen más probabilidades de cumplir de forma constante sus SLA

42% Vs. **22%**

Por posición:



* Nota: No recomendamos informar sobre estadísticas con una base inferior a 30

Sección 5: Complejidad, cultura y lo que viene

Barreras organizativas y planes de inversión futuros

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

Principales desafíos:

Falta de personal cualificado	44%
Entorno informático complejo	41%
Fragmentación de proveedores/herramientas	37%
Limitaciones presupuestarias	30%
Baja priorización ejecutiva	14%

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

35%	5.000 o más empleados
41%	3.000-4.999 empleados
46%	1.000-2.999 empleados

56%

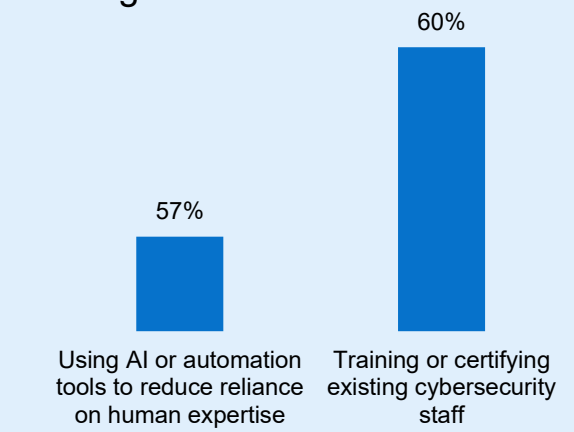
Piensa que la dirección sobreestima la preparación de su organización ante un gran evento cibernético

99%

Reconoce que tienen carencias en sus habilidades o experiencia en ciberseguridad

PERO...

Las organizaciones actúan a través de:



Mirando hacia las inversiones

#1

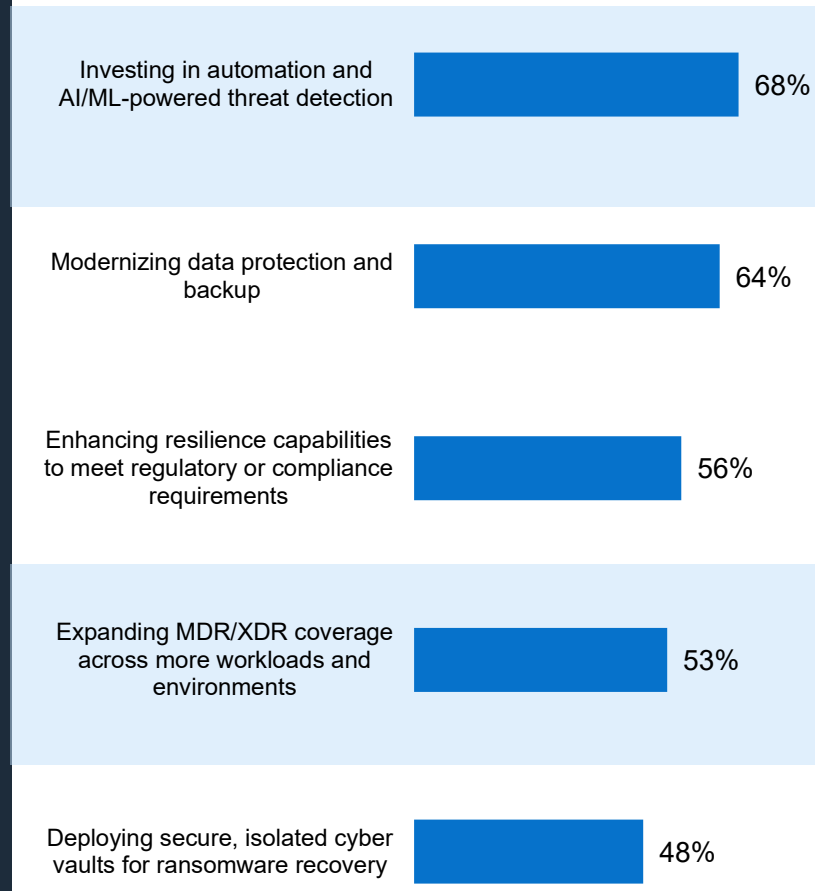
El motor de la inversión es el panorama de amenazas en evolución

97%

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

Camino a seguir para mantener una postura madura: Inversión continua y Optimización

Priorizamos las inversiones en resiliencia cibernética durante los próximos 12 meses



Las organizaciones maduras y resilientes cibernéticas están invirtiendo continuamente