COHESITY

INFORME DE RESILIENCIA CIBERNÉTICA

Preparada para el riesgo o expuesta al riesgo: La brecha de resiliencia cibernética en organizaciones medianas

MAYO DE 2026

Todos hablan sobre la detección y la prevención de ataques cibernéticos, pero los titulares narran una historia diferente. La prevención y la detección por sí solas ya no son suficientes. Incluso las organizaciones más avanzadas están sufriendo interrupciones devastadoras que se propagan desde las operaciones de TI hasta la sala de juntas, y más allá.

Para comprender por qué, y qué separa a las organizaciones resilientes de las que aún tienen dificultades, Cohesity encuestó a 3200 responsables de la toma de decisiones en Operaciones de TI y Seguridad en 11 países. Entre ellos, había casi 1000 participantes de organizaciones medianas. Sus respuestas revelan una brecha de resiliencia cada vez mayor entre las organizaciones preparadas para el riesgo, que pueden recuperarse de forma rápida y con confianza, y sus pares expuestos al riesgo, que siguen siendo vulnerables a interrupciones prolongadas y al daño financiero posterior.

Nuestra investigación examina los impactos en el mundo real de los ciberataques materiales, cómo las organizaciones medianas autoevaluaron su resiliencia cibernética frente a las mejores prácticas y los pasos que tomaron para detectar, responder y recuperarse de estos incidentes. También destaca lo que aprendieron y cómo recurren a la IA y la automatización para acelerar la resiliencia y cerrar la brecha.

CIBERATAQUES SIGNIFICATIVOS:
LA NUEVA REALIDAD DE LOS NEGOCIOS MODERNOS

Los incidentes cibernéticos no son iguales. Muchas organizaciones gestionan intentos de phishing de rutina, sondeos de malware o interrupciones del sistema casi todos los días. Pero los ciberataques significativos son diferentes. Nuestra encuesta definió un ciberataque significativo como un incidente que ocasionó un impacto financiero, reputacional, operativo o de pérdida de clientes medible.

PARA LAS ORGANIZACIONES MEDIANAS, ESTOS ATAQUES DE ALTO IMPACTO YA NO SON EVENTOS AISLADOS.

75 %

de los encuestados han experimentado al menos un ciberataque significativo.

55 %

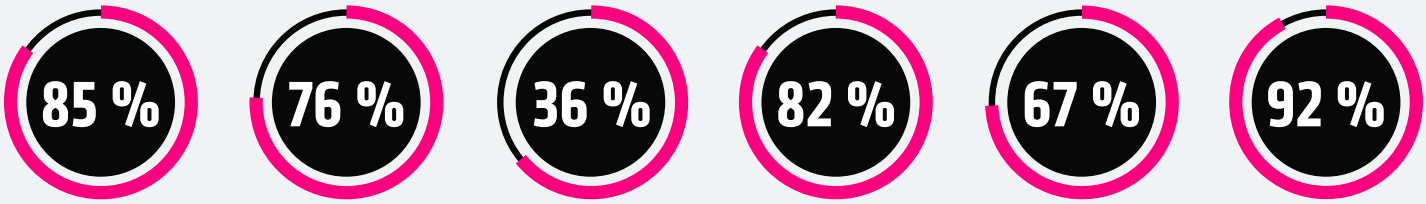
experimentó uno en los últimos 12 meses.

25 %

sufrió múltiples incidentes durante el período de 12 meses.

EL COSTO REAL DE LOS CIBERATAQUES SIGNIFICATIVOS

LAS PRESIONES FINANCIERAS Y REGULATORIAS TAMBIÉN SE HICIERON ECO EN LAS ORGANIZACIONES MEDIANAS QUE ENCUESTAMOS:



reportó pérdida de ingresos

de las organizaciones que cotizan en bolsa informaron haber revisado sus previsiones financieras[1]

clientes perdidos

pagó un rescate, con un promedio de 1,3 millones de dólares estadounidenses por incidente.

de las organizaciones de capital privado reasignaron su presupuesto, alejándose de las iniciativas de crecimiento

enfrentó consecuencias legales o regulatorias, incluidas multas regulatorias (46 %) y demandas o litigios colectivos (33 %)

[1] Si bien relativamente pocas empresas que cotizan en bolsa han divulgado formalmente revisiones de ganancias tras un incidente cibernético, estos hallazgos sugieren que los efectos financieros y operativos se extienden mucho más allá de lo que revelan las presentaciones públicas.

CONFIANZA FRENTE A LAS CONSECUENCIAS

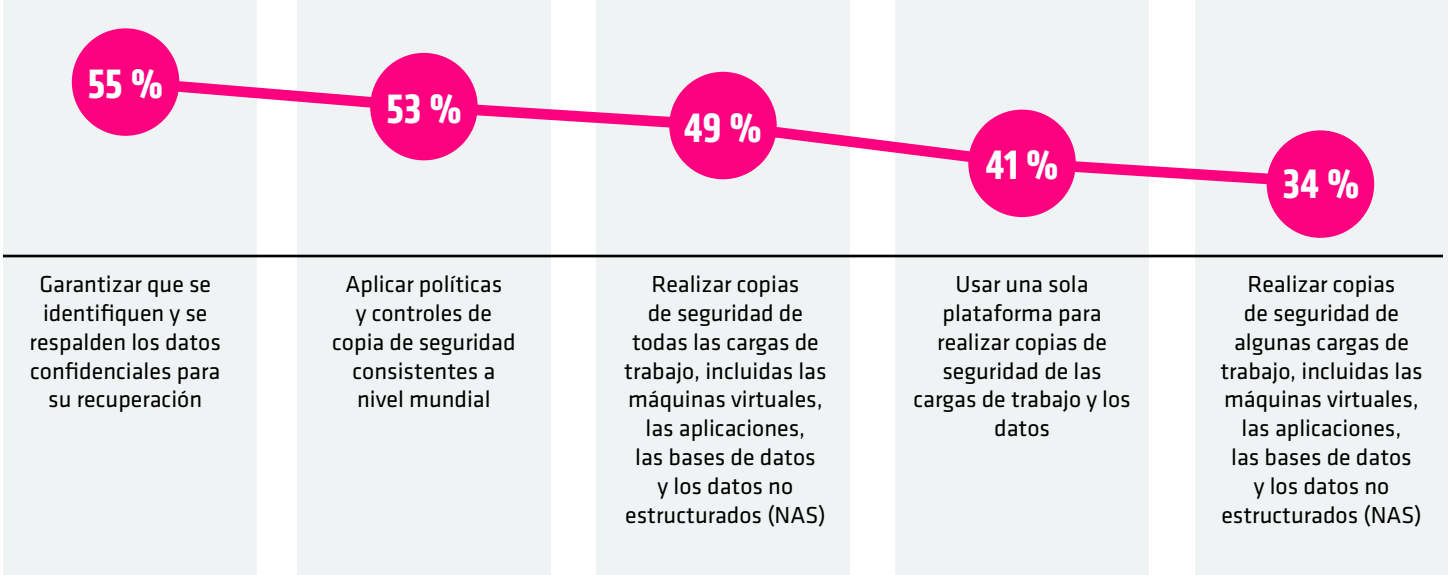
Dada la escala de las consecuencias financieras y operativas reveladas en nuestra investigación, se podría esperar una preocupación generalizada sobre la resiliencia organizacional. Sin embargo, muchos encuestados (47 %) expresaron plena confianza en que su estrategia de resiliencia cibernética podría resistir las amenazas actuales. Este nivel de confianza contrasta considerablemente con los impactos significativos que muchas de estas mismas organizaciones han sufrido.

QUÉ ESTÁN HACIENDO (Y NO ESTÁN HACIENDO) LAS ORGANIZACIONES

Queríamos mirar bajo la superficie y descubrir dónde existen brechas de resiliencia. Para ello, les pedimos a los encuestados que describieran su enfoque de algunas de las prácticas y capacidades clave asociadas con cinco dimensiones centrales de la resiliencia cibernética: **protección de datos, recuperación de datos, detección e investigación de amenazas, resiliencia de las aplicaciones** y **optimización de la postura de riesgo de los datos.**

LA PROTECCIÓN DE DATOS PERMANECE FRAGMENTADA EN ENTORNOS HÍBRIDOS Y MULTINUBE

¿Qué hace su organización para proteger todos los datos en entornos híbridos y/o multinube?



Un poco más de la mitad de las organizaciones medianas garantizan que se identifiquen y se respalden los datos confidenciales para su recuperación. Aproximadamente la misma proporción aplica políticas y controles de copia de seguridad consistentes a nivel mundial. Menos de la mitad realiza copias de seguridad de todas las cargas de trabajo o usa una sola plataforma para proteger las cargas de trabajo y los datos. Un tercio realiza copias de seguridad solo de cargas de trabajo seleccionadas. Esta fragmentación limita la visibilidad y la consistencia en todos los entornos. La resiliencia cibernética madura depende de unificar la copia de seguridad y la recuperación dentro de una sola plataforma inteligente asegurada por los principios de Confianza Cero.

LAS MEDIDAS DE RECUPERACIÓN DE DATOS SON COMUNES, PERO LA MADUREZ VARÍA

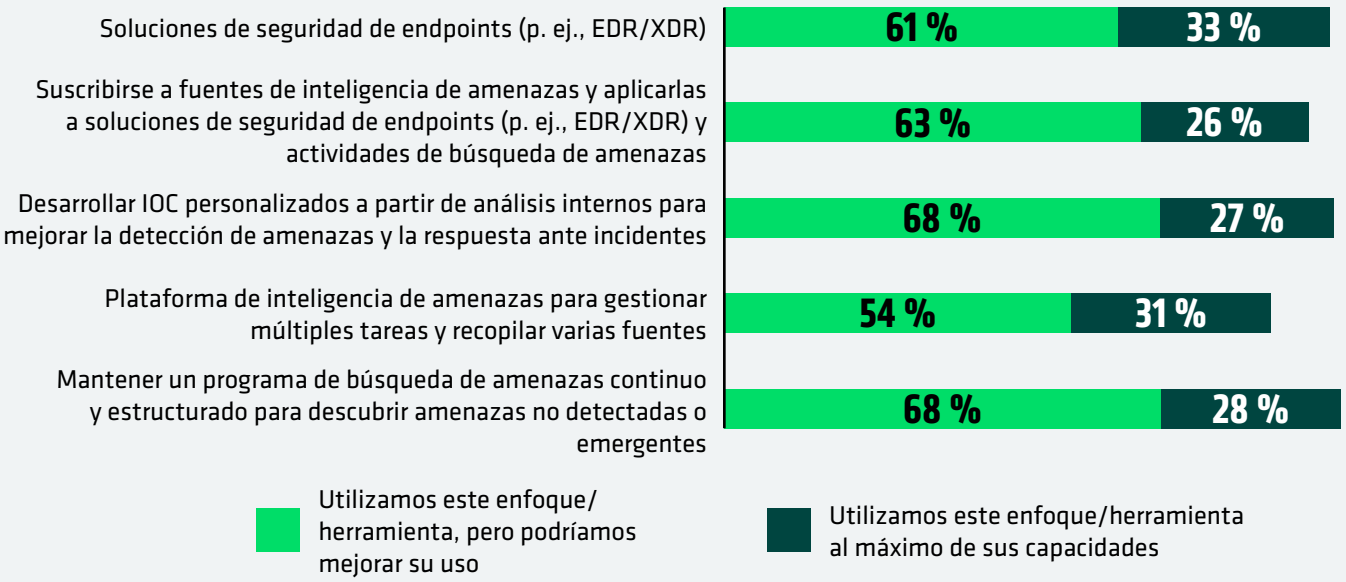
¿Qué hace su organización para garantizar que sus datos siempre sean recuperables?

60 %	Requiere autorización adicional en tareas administrativas de alto riesgo asociadas con soluciones de copia de seguridad y recuperación
53 %	Autenticación multifactor en nuestra solución de copia de seguridad
47 %	Seguir la “regla 3-2-1 de copias de seguridad” (tres copias de datos, almacenadas en dos tipos de medios diferentes, con una copia guardada fuera del sitio)
42 %	Proteger los datos críticos con inmutabilidad
38 %	Derechos de acceso de mínimo privilegio en las cargas de trabajo respaldadas

Muchas organizaciones medianas han fortalecido los controles de acceso en relación a los entornos de copia de seguridad, y más de la mitad requiere autorización adicional de administrador para tareas de alto riesgo. Alrededor de la mitad aplica la autenticación multifactor y cerca de la mitad sigue la regla 3-2-1 de copias de seguridad. Menos organizaciones protegen los datos críticos con inmutabilidad o aplican derechos de acceso con privilegios mínimos. Estas brechas hacen que la recuperación total sea menos segura. La resiliencia cibernética madura depende de copias de recuperación verificadas, aisladas y a prueba de manipulaciones.

LAS HERRAMIENTAS DE DETECCIÓN E INVESTIGACIÓN DE AMENAZAS NO SE UTILIZAN LO SUFICIENTE

¿En qué medida utiliza su organización cada uno de los siguientes métodos o herramientas para detectar e investigar amenazas?



Las herramientas de detección e investigación de amenazas están ampliamente implementadas, pero no se utilizan lo suficiente. La mayoría de las organizaciones medianas utilizan seguridad de endpoints, fuentes de inteligencia de amenazas, IOC personalizados, plataformas de inteligencia de amenazas y programas estructurados de búsqueda de amenazas, pero solo una minoría aprovecha estas herramientas al máximo de su potencial. La resiliencia cibernética madura depende de integrar estas herramientas en un bucle de inteligencia continuo que mejore la visibilidad, la detección y la respuesta.

LAS MEDIDAS DE RESILIENCIA INCOMPLETAS AUMENTAN EL RIESGO DE REINFECCIÓN

¿Qué hace/haría su organización para garantizar la resiliencia de las aplicaciones frente a ataques cibernéticos?

57 % Identificar y remediar las brechas de control de seguridad antes de restaurar los sistemas a la producción

60 % Realizar ensayos simulados anuales de extremo a extremo, incluido un equipo multifuncional de partes interesadas técnicas, legales, estratégicas, ejecutivas y de comunicaciones.

56 % Usar un repositorio en línea en una bóveda de los sistemas e información críticos para permitir la respuesta y la recuperación ante incidentes

47 % Usar un entorno aislado para la investigación de incidentes, la remediación y la recuperación segura

33 % Inmutabilidad para todos los datos de respaldo

Las organizaciones medianas están avanzando en su enfoque hacia la resiliencia de las aplicaciones, pero aún quedan brechas. La mayoría identifica brechas en los controles de seguridad antes de restaurar los sistemas. Una proporción comparable mantiene repositorios protegidos en línea. Más de la mitad también realiza ensayos anuales de recuperación. Una cantidad menor utiliza entornos aislados para la investigación y recuperación seguras. Un porcentaje aún menor aplica la inmutabilidad a todos los datos de respaldo. Estas brechas dejan los procesos de recuperación vulnerables a la reinfección o la pérdida de datos. La resiliencia cibernética madura combina la preparación con zonas de recuperación seguras y verificables.

LA CLASIFICACIÓN DE DATOS GANA TERRENO A MEDIDA QUE SE EXPANDE EL USO DEL RIESGO

¿Cómo utiliza su organización los enfoques/herramientas de descubrimiento y clasificación de datos para minimizar la exposición al riesgo de los datos en todo su entorno de datos?

Identificar y resolver las brechas de privacidad y seguridad de los respaldos para el cumplimiento

Usar la clasificación de datos de respaldo para determinar las obligaciones de cumplimiento de los datos afectados

Definir y comprender la materialidad de un ciberataque antes de que ocurra un incidente

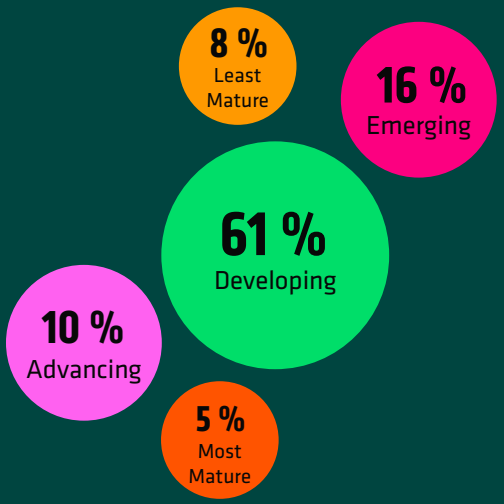
Identificar y priorizar los sistemas para el respaldo

Las organizaciones medianas están utilizando el descubrimiento y la clasificación de datos de manera más estratégica en materia de cumplimiento, respuesta y recuperación. Casi dos tercios abordan las infracciones de privacidad y seguridad, mientras que más de la mitad utiliza la clasificación para guiar el cumplimiento durante un ataque. Más de la mitad también define la significancia antes de un incidente y prioriza los respaldos en función de los riesgos. La resiliencia cibernética madura transforma la clasificación en un enfoque sistemático que optimiza la postura de riesgo de los datos y posibilita la protección, la respuesta y la recuperación.

UNA IMAGEN MÁS CLARA DE LA MADUREZ DE LA RESILIENCIA

Al puntuarse en conjunto, las respuestas de los encuestados sirvieron como un barómetro de alto nivel de la madurez de la resiliencia cibernética, revelando patrones claros sobre cómo las organizaciones de tamaño mediano están construyendo –o tienen dificultades para construir– resiliencia en la práctica. Si bien la mayoría se encuentra en la etapa de desarrollo, solo el 5 % demuestra las capacidades más maduras e integradas que definen a las organizaciones preparadas para el riesgo.

LA CURVA DE MADUREZ DE LA RESILIENCIA CIBERNÉTICA



Menos madura (8 %): Las copias de seguridad, las políticas y las salvaguardas de seguridad están en gran medida ausentes o son inconsistentes. La autenticación multifactor (MFA) y los controles administrativos rara vez se aplican, la recuperación suele carecer de aislamiento y las evaluaciones de cumplimiento o materialidad normalmente se pasan por alto.

Emergente (16 %): Existen algunas prácticas de resiliencia, pero de manera inconsistente. Puede que las organizaciones hagan copias de seguridad de datos confidenciales, apliquen políticas globales o usen la MFA, pero rara vez en combinación. Existen esfuerzos de inteligencia de amenazas y cumplimiento, pero siguen siendo inmaduros y fragmentados.

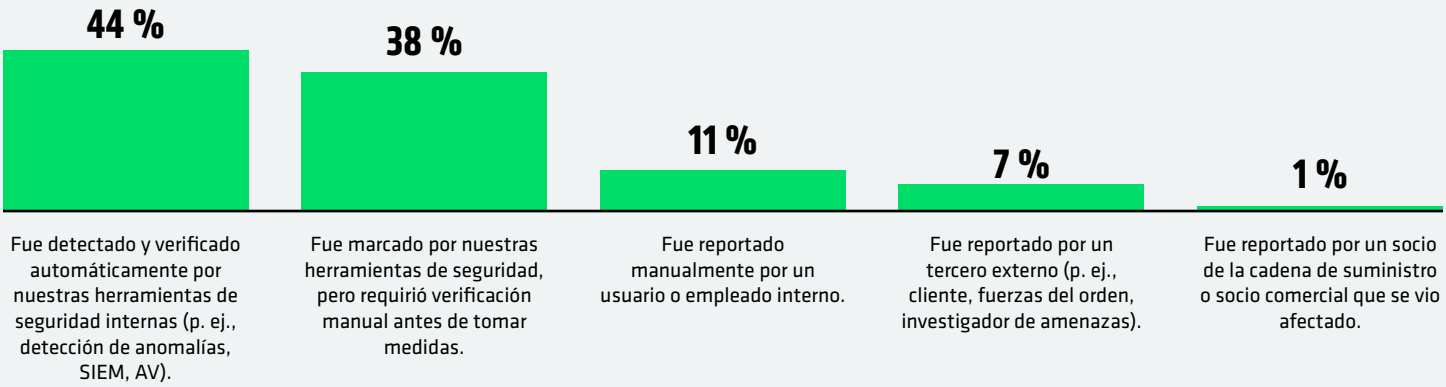
En desarrollo (61%): Las prácticas centrales, como las copias de seguridad, los controles administrativos y la inteligencia de amenazas, son más comunes, aunque aún son desiguales. Los entornos de recuperación, las verificaciones de cumplimiento y la remediación de brechas de seguridad se aplican esporádicamente, lo que genera que los esfuerzos de resiliencia sean parcialmente efectivos.

Avanzando (10 %): La mayoría de las prácticas clave se aplican de manera constante, incluidas las políticas globales de respaldo, las aprobaciones administrativas y la remediación antes de la recuperación. Se utiliza la inteligencia de amenazas, pero no está completamente optimizada, y persisten algunas brechas en torno a la recuperación aislada y la cobertura completa de cumplimiento.

Más madura (5 %): La resiliencia es sistémica e integral. Los datos confidenciales se respaldan globalmente, la MFA y los controles administrativos son estándar, se maximiza la inteligencia de amenazas, la recuperación se asegura mediante la remediación y las salvaguardas de cumplimiento se cumplen de manera constante.

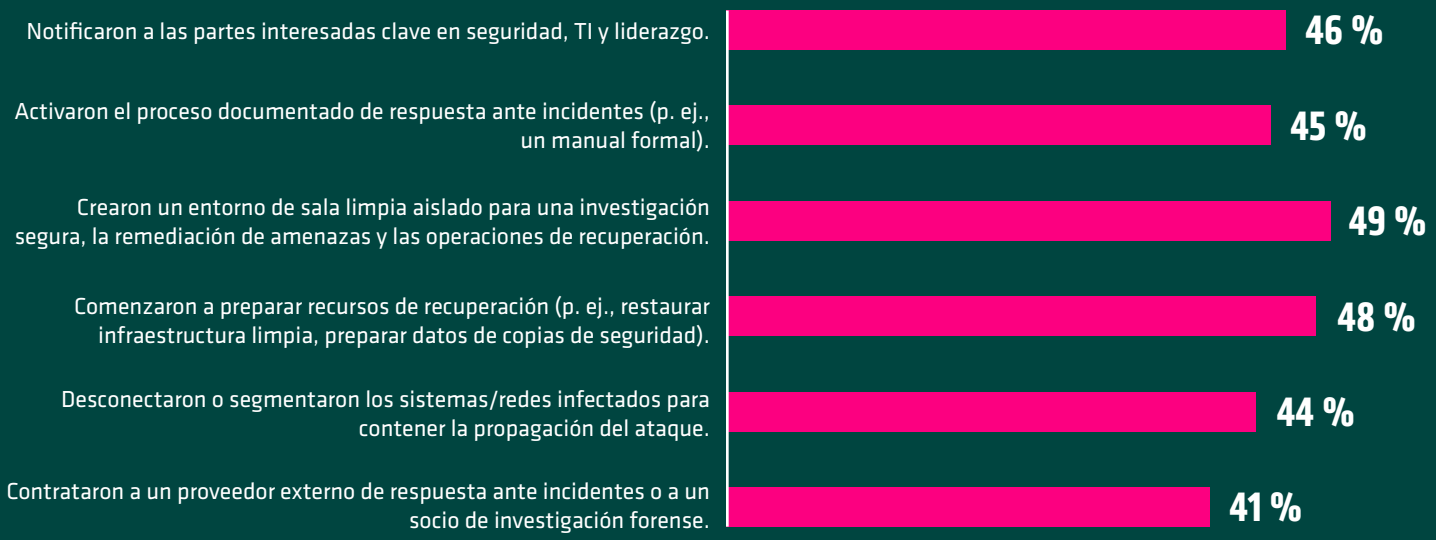
RESILIENCIA BAJO PRESIÓN

CÓMO LOS EQUIPOS IDENTIFICARON EL ATAQUE



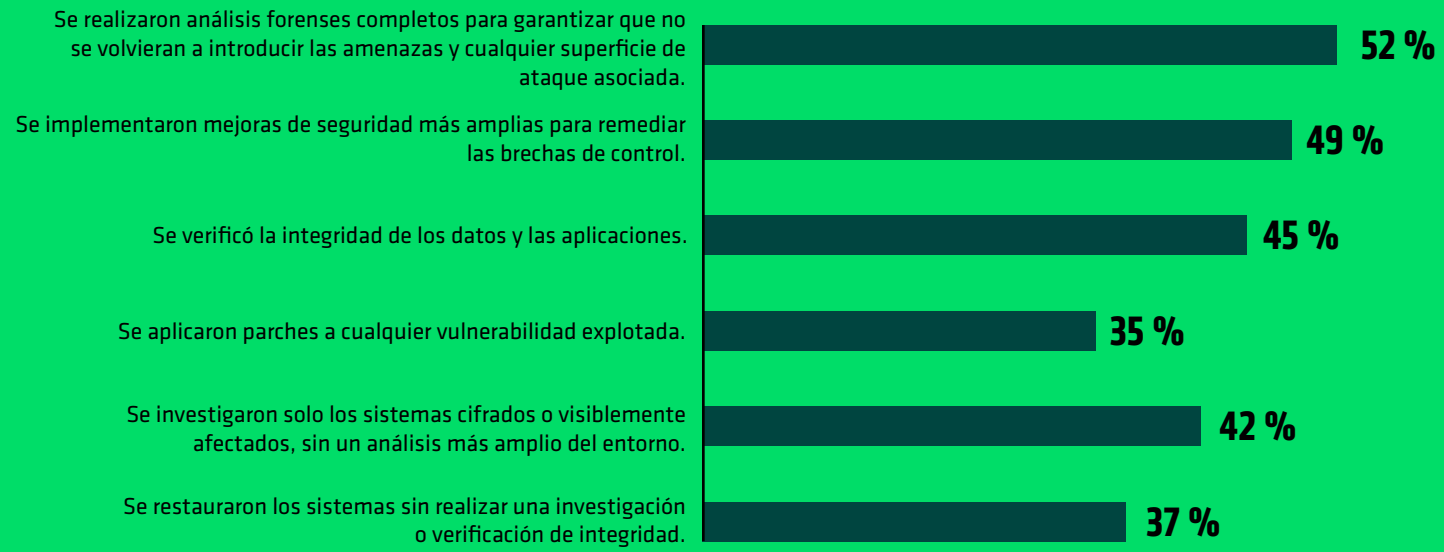
En caso de un ataque cibernético, la mayoría de las organizaciones medianas detectan los incidentes internamente, y la mayor parte se identifica automáticamente y se verifica con herramientas de seguridad. Muchos otros son marcados por herramientas, pero requieren verificación manual antes de tomar medidas. Muchos menos incidentes son reportados por empleados o terceros. La detección está impulsada en gran medida por herramientas, aunque la validación humana aún desempeña un papel importante.

ACCIONES QUE LOS EQUIPOS TOMARON DESPUÉS DE CONFIRMAR EL ATAQUE



Después de confirmar un ataque, las organizaciones medianas tomaron una serie de medidas para contener la amenaza y comenzar la recuperación. Un porcentaje similar comenzó a preparar recursos de recuperación, crear entornos de sala limpia aislados, notificar a las partes interesadas clave, desconectar los sistemas infectados y activar manuales de respuesta. Se involucraron ligeramente menos socios externos de respuesta ante incidentes. Estos patrones sugieren que los esfuerzos de respuesta se adoptan ampliamente, pero aún no están completamente estandarizados para todas las acciones críticas.

PASOS TOMADOS ANTES DE VOLVER A PONER LOS SISTEMAS Y LOS DATOS EN LÍNEA



Antes de volver a poner en línea los sistemas y los datos, las organizaciones medianas emplearon una combinación de medidas forenses y correctivas. Alrededor de la mitad realizó análisis forenses completos, implementó mejoras de seguridad más amplias o verificó la integridad de los datos y las aplicaciones, mientras que cifras similares se centraron solo en los sistemas visiblemente afectados. Una proporción menor aplicó parches a las vulnerabilidades explotadas o restauró los sistemas sin investigación ni verificación. Estas brechas pueden aumentar el riesgo de reinfección o exposición residual.

DESAFÍOS QUE ENFRENTARON LOS EQUIPOS DURANTE EL ATAQUE

51 %

Incapacidad para comunicarse o coordinarse dentro de nuestro equipo debido a que los sistemas críticos estaban fuera de servicio (p. ej., correo electrónico, aplicaciones colaborativas, gestión de tickets).

47 %

Presión del liderazgo para restaurar los sistemas antes de que se remediara el ataque.

41 %

Se evadieron las herramientas de seguridad y se atacaron las copias de seguridad.

40 %

Nos recuperamos, pero luego fuimos reinfectados porque las amenazas no se erradicaron por completo.

37 %

Falta de acceso a puntos de recuperación limpios y validados.

Los equipos enfrentaron una variedad de desafíos operativos y técnicos durante el ataque. Alrededor de la mitad tuvo dificultades para comunicarse mientras los sistemas estaban caídos o sintió presión para restaurar los sistemas antes de que se completara la remediación. Los equipos también informaron evasión de herramientas de seguridad, copias de seguridad atacadas, reinfección después de la recuperación o falta de acceso a puntos de recuperación limpios. Estos desafíos dejan al descubierto brechas en la preparación que pueden complicar la respuesta y prolongar la interrupción.

DÓNDE LA INVERSIÓN EN RESILIENCIA SIGUE SIENDO INSUFICIENTE

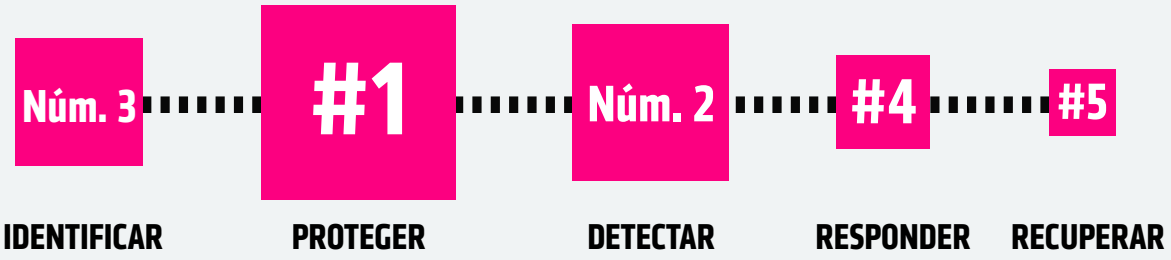
Incluso las organizaciones bien preparadas luchan por mantener la resiliencia una vez que se desarrolla un ataque. A medida que aumenta la presión operativa, las brechas de coordinación, la remediación incompleta y los riesgos de reinfección exponen cuán frágil puede ser la recuperación sin procesos unificados y garantía continua.

Estos patrones reflejan cómo las organizaciones medianas asignan sus presupuestos de resiliencia cibernética hoy en día. Les preguntamos a los encuestados cómo distribuyen el gasto entre las cinco funciones principales del Marco de Ciberseguridad del NIST: Identificar, Proteger, Detectar, Responder y Recuperar.

La mayoría continúa invirtiendo fuertemente en prevención, protección y detección, mientras que, comparativamente, menos financiamiento respalda la respuesta y la recuperación verificada. El resultado es una curva de madurez que todavía se inclina hacia la defensa en lugar de la restauración, lo que destaca una oportunidad sin explotar de fortalecer la resiliencia donde más importa: después del ataque.

MARCO DE CIBERSEGURIDAD DEL NIST.

El tamaño del cuadro muestra la proporción de inversiones en resiliencia cibernética, de mayor a menor.



LA IA Y LA AUTOMATIZACIÓN EMERGEN COMO MULTIPLICADORES DE RESILIENCIA

Los resultados también muestran que las organizaciones medianas ven a la IA como un poderoso facilitador de resiliencia cibernética, particularmente para mejorar la velocidad de detección y la precisión de la respuesta. Casi todos los encuestados calificaron herramientas como la detección de anomalías, el análisis del comportamiento del usuario y la investigación y respuesta ante amenazas impulsadas por IA como eficaces para fortalecer su postura de seguridad.

Incluso los asistentes más nuevos basados en GenAI, capaces de realizar consultas sobre amenazas en lenguaje natural y análisis contextual, están ganando terreno como una forma de simplificar y acelerar la toma de decisiones. El 56% de las organizaciones medianas dijo que una de las mayores lecciones aprendidas después de un ataque cibernético era la necesidad de una mayor automatización en la detección, la respuesta y la recuperación. Esto refleja la creciente demanda de plataformas integradas de automatización y orquestación, donde la IA actúa como un multiplicador de fuerza, impulsando una mayor eficiencia, consistencia y efectividad en todos estos procesos.

Al mirar hacia el futuro, la mayoría espera que la IA desempeñe un papel cada vez más estratégico en la defensa cibernética para fines de 2026. El 56 % anticipa que la IA apoyará la toma de decisiones humanas, mejorando el análisis y las recomendaciones, y que los seres humanos seguirán teniendo el control de las acciones finales. El 37 % espera que la IA se convierta en un factor central para la detección y la respuesta, e incluso que tome algunas decisiones autónomas. Esto indica una trayectoria clara: La IA está evolucionando de asistente a piedra angular operativa de la resiliencia cibernética, y está preparada para mejorar la velocidad, la precisión y la confianza en la detección, la respuesta y la recuperación.

EL FUTURO DE LA RESILIENCIA COMIENZA AHORA

Si bien las organizaciones medianas están logrando un progreso medible en la resiliencia cibernética, muchas aún tienen margen para mejorar su respuesta, recuperación y validación de la preparación después de un ataque. La resiliencia cibernética representa una enorme ventaja competitiva. El futuro pertenece a las organizaciones que invierten en las personas, los productos y los procesos para recuperarse más rápido, mantener la confianza del cliente y mantener el negocio en marcha cuando otros no pueden. Cuando la disrupción es prácticamente inevitable, la resiliencia no es solo protección; es desempeño.

Desarrolle resiliencia antes de que se produzca una crisis:

- Obtenga información sobre las soluciones de resiliencia cibernética de Cohesity para organizaciones medianas.
- Evalúe la madurez de su resiliencia cibernética con esta tarjeta de evaluación de resiliencia
- Suba de nivel con un plan de acción de resiliencia cibernética de cinco pasos

METODOLOGÍA

Cohesity encargó a Vanson Bourne que encuestara a 3200 responsables de la toma de decisiones de TI y seguridad en septiembre de 2025, lo que constituye la base de estos hallazgos. Los encuestados representan a organizaciones en EE. UU. (500), Brasil (200), Reino Unido (400), Alemania (400), Francia (400), EAU/ Arabia Saudita (100), Australia (200), Corea del Sur (200), Japón (400), India (200) y Singapur (200). Las organizaciones tenían 1000 empleados o más y provenían de una variedad de sectores públicos y privados, con un enfoque en los servicios financieros, el sector público y la atención médica.

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

2000049-001-ES-LA 7-2026