COHESITY

INFORME DE CIBERRESILIENCIA

Preparados para el Riesgo o Expuestos al Riesgo: La Brecha de Ciberresiliencia en los Servicios Financieros

MAYO DE 2026

Todo el mundo habla de detectar y prevenir los ciberataques, pero los titulares cuentan una historia diferente. La prevención y la detección por sí solas ya no son suficientes. Incluso las organizaciones más avanzadas están sufriendo graves interrupciones que se extienden desde las operaciones de TI hasta la junta directiva, e incluso más allá.

Para comprender las razones y qué diferencia a las organizaciones resilientes de aquellas 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 se encontraban 390 participantes de organizaciones de servicios financieros. Sus respuestas revelan una brecha de resiliencia cada vez mayor entre las organizaciones de servicios financieros preparadas para el riesgo, capaces de recuperarse con rapidez y confianza, y sus pares expuestos al riesgo, que permanecen vulnerables a interrupciones prolongadas y a daños financieros derivados.

Nuestra investigación examina los impactos reales de los ciberataques materiales, la forma en que las organizaciones de servicios financieros autoevaluaron su ciberresiliencia frente a las mejores prácticas, y las medidas que adoptaron para detectar estos incidentes, responder a ellos y recuperarse de los mismos. También destaca lo que aprendieron y cómo están recurriendo a la IA y la automatización para acelerar la resiliencia y cerrar la brecha.

CIBERATAQUES MATERIALES:
LA NUEVA REALIDAD DE LOS NEGOCIOS MODERNOS

No todos los incidentes cibernéticos son iguales. Muchas organizaciones de servicios financieros gestionan intentos rutinarios de phishing, sondeos de malware o interrupciones del sistema casi a diario. Pero los ciberataques contra materiales son diferentes. Nuestra encuesta definió un ciberataque significativo como un incidente que causó un impacto cuantificable en terminos financieros, reputacionales, operativos o de pérdida de clientes.

ESTOS ATAQUES DE ALTO IMPACTO YA NO SON EVENTOS AISLADOS PARA LAS ORGANIZACIONES DE SERVICIOS FINANCIEROS.

77%

de los encuestados ha sufrido al menos un ciberataque importante

57%

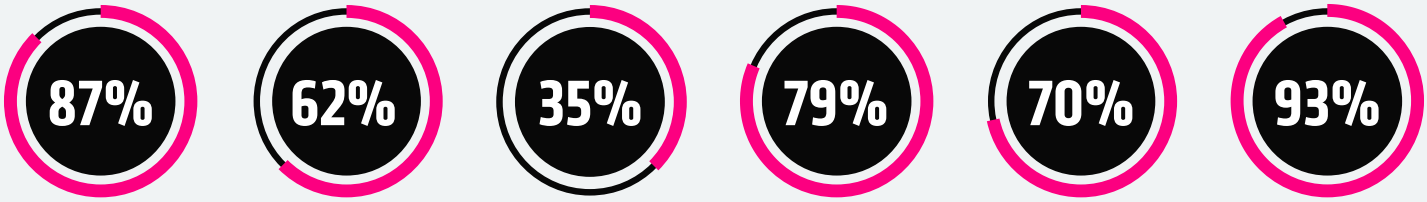
experimentó uno en los últimos 12 meses

27%

sufrió múltiples incidentes durante el período de 12 meses

EL COSTE REAL DE LOS CIBERATAQUES MATERIALES

LAS PRESIONES FINANCIERAS Y REGULATORIAS RESONARON EN LAS ORGANIZACIONES DE SERVICIOS FINANCIEROS QUE ENCUESTAMOS:



reportó pérdidas de ingresos

de las empresas que cotizan en bolsa informó haber revisado sus previsiones financieras[1]

perdió clientes

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

de las organizaciones privadas reasignaron presupuesto, desviándolo de las iniciativas de crecimiento

se enfrentó a consecuencias legales o regulatorias, incluidas multas regulatorias (51%) y demandas o litigios colectivos (41%)

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

CONFIANZA FRENTE A LAS CONSECUENCIAS

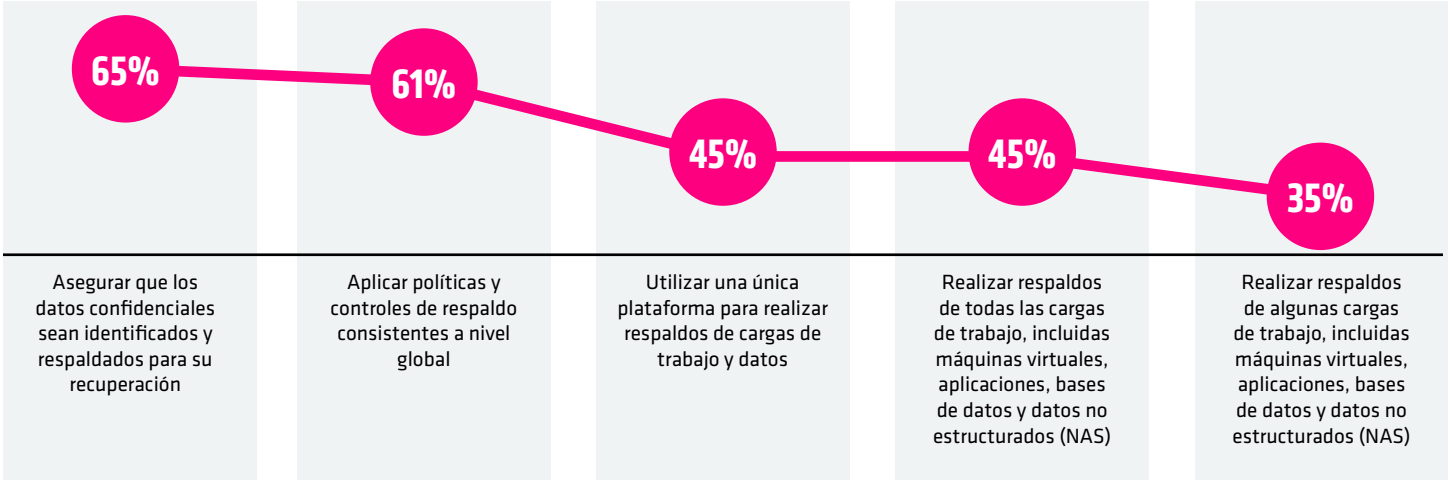
Dada la magnitud de las consecuencias financieras y operativas reveladas en nuestra investigación, cabría esperar una preocupación generalizada por la resiliencia de las organizaciones. Sin embargo, casi la mitad de los encuestados (46%) expresó plena confianza en que su estrategia de ciberresiliencia podría resistir las amenazas actuales. Este nivel de confianza contrasta marcadamente con las importantes repercusiones materiales que muchas de estas mismas organizaciones han sufrido.

LO QUE LAS ORGANIZACIONES ESTÁN HACIENDO (Y LO QUE NO ESTÁN HACIENDO)

Queríamos ir más allá de la superficie y descubrir dónde existen deficiencias en la resiliencia. Para ello, pedimos a los encuestados que describieran su enfoque respecto a algunas de las prácticas y capacidades clave asociadas a cinco dimensiones fundamentales de la ciberresiliencia: **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 SIGUE FRAGMENTADA EN ENTORNOS HÍBRIDOS Y MULTINUBE.

¿Cuál de las siguientes acciones realiza su organización para proteger todos los datos en entornos híbridos y/o multinube?



Casi dos tercios de las organizaciones de servicios financieros garantizan que los datos confidenciales sean identificados y respaldados para su recuperación, mientras que un porcentaje ligeramente menor aplica políticas de respaldo consistentes a nivel global. Menos de la mitad realiza copias de seguridad de todas las cargas de trabajo o depende de una única plataforma. Alrededor de un tercio realiza respaldos únicamente de cargas de trabajo seleccionadas. Esta fragmentación limita la visibilidad y la coherencia entre los distintos entornos. Una ciberresiliencia madura depende de la unificación de la copia de seguridad y la recuperación dentro de una única plataforma inteligente protegida por los principios de confianza cero (Zero Trust).

LAS MEDIDAS DE RECUPERABILIDAD DE DATOS SON COMUNES, PERO SU GRADO DE MADUREZ VARÍA.

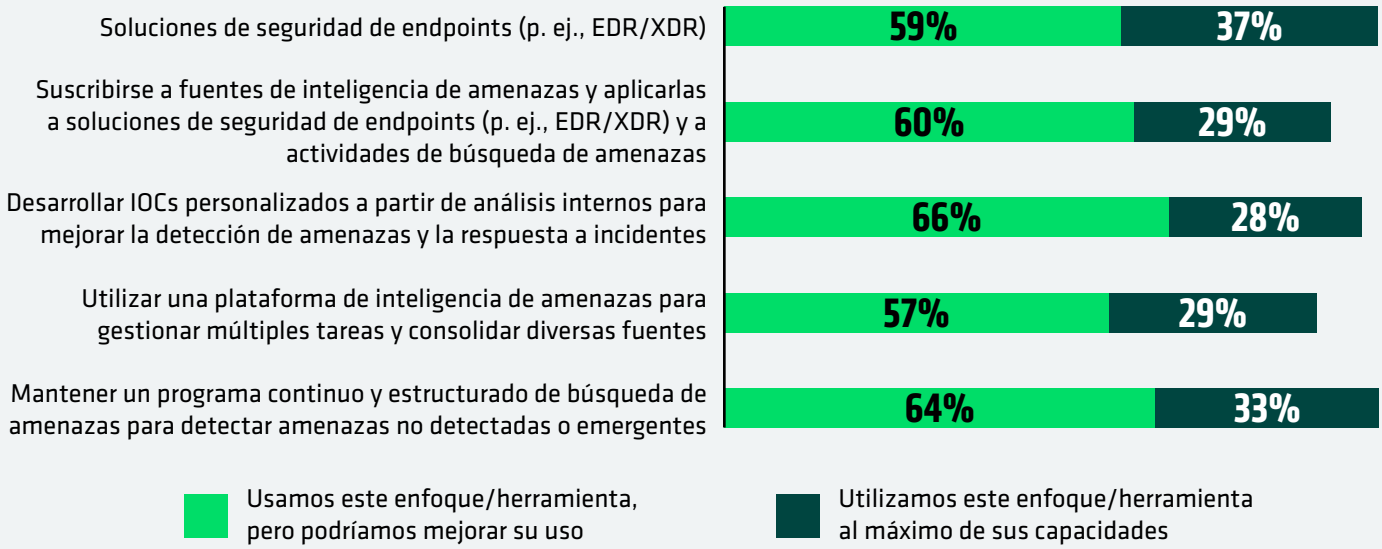
¿Qué hace su organización para garantizar que sus datos sean siempre recuperables?

64%	Exigir autorización adicional para las tareas administrativas de alto riesgo asociadas a las soluciones de respaldo y recuperación
61%	Autenticación multifactor en su solución de respaldo
48%	Seguir la “regla de respaldo 3-2-1” (tres copias de los datos, almacenadas en dos tipos de medios diferentes, con una copia guardada fuera de las instalaciones)
45%	Proteger los datos críticos con inmutabilidad
41%	Aplicar principios de acceso de privilegio mínimo en las cargas de trabajo respaldadas

Muchas organizaciones de servicios financieros han reforzado los controles de acceso en torno a los entornos de respaldo; casi dos tercios exigen una autorización administrativa adicional para tareas de alto riesgo, y poco más de la mitad implementa la autenticación multifactor. Casi la mitad sigue la regla de respaldo 3-2-1 y poco menos de la mitad protege los datos críticos mediante inmutabilidad, mientras que una proporción menor aplica derechos de acceso de privilegio mínimo. Estas deficiencias hacen que la recuperación total sea menos segura. Una ciberresiliencia madura depende de copias de recuperación verificadas, aisladas e inalterables.

LAS HERRAMIENTAS DE DETECCIÓN E INVESTIGACIÓN DE AMENAZAS ESTÁN INFRAUTILIZADAS

¿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 desplegadas, pero a menudo no se utilizan lo suficiente. La mayoría de las organizaciones de servicios financieros utilizan seguridad de puntos finales, fuentes de inteligencia sobre amenazas y programas estructurados de búsqueda de amenazas; sin embargo, solo una minoría aprovecha estas herramientas en todo su potencial. La adopción de capacidades avanzadas, tales como los indicadores de compromiso (IOC) personalizados y las plataformas de inteligencia de amenazas, sigue siendo particularmente limitada. Una ciberresiliencia madura depende de la integración de estas herramientas en un ciclo de inteligencia continuo que mejore la visibilidad, la detección y la respuesta.

LAS ORGANIZACIONES SON VULNERABLES A LA REINFECCIÓN

¿Qué hace, o qué haría, su organización para garantizar la resiliencia de las aplicaciones frente a los ciberataques?

64% Realizar simulacros anuales de extremo a extremo, los cuales incluyen un equipo multifuncional compuesto por partes interesadas de las áreas técnica, legal, estratégica, ejecutiva y de comunicaciones

61% Identificar y subsanar las brechas en los controles de seguridad antes de restaurar los sistemas a producción

60% Mantener un repositorio en línea y seguro de sistemas críticos e información para respaldar la respuesta a incidentes y la recuperación

51% Utilizar un entorno aislado para la investigación de incidentes, la remediación y la recuperación segura

39% Aplicar inmutabilidad para todos los datos de respaldo

Las organizaciones de servicios financieros están avanzando en su enfoque hacia la resiliencia de las aplicaciones, pero persisten las brechas. Poco más de la mitad identifica las brechas en los controles de seguridad antes de restaurar los sistemas, mientras que casi dos tercios realizan simulacros anuales de recuperación. Alrededor de seis de cada diez mantienen repositorios en línea y en bóvedas, y poco más de la mitad utiliza entornos aislados para la investigación y recuperación seguras. Menos de la mitad aplica la inmutabilidad a todos los datos de respaldo. Estas deficiencias hacen que los procesos de recuperación sean vulnerables a la reinfección o a la pérdida de datos. Una ciberresiliencia madura combina la preparación con zonas de recuperación seguras y verificables.

LA CLASIFICACIÓN DE DATOS COBRA IMPULSO, PERO SU USO BASADO EN RIESGOS SIGUE EVOLUCIONANDO

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

67%

Identificar y resolver las infracciones de privacidad y seguridad de las copias de seguridad para garantizar el cumplimiento normativo

62%

Durante un ciberataque, utilizamos la clasificación de datos de respaldo para determinar las obligaciones de cumplimiento de los datos afectados

59%

Definir y comprender la materialidad de los ciberataques antes de que ocurra un incidente

56%

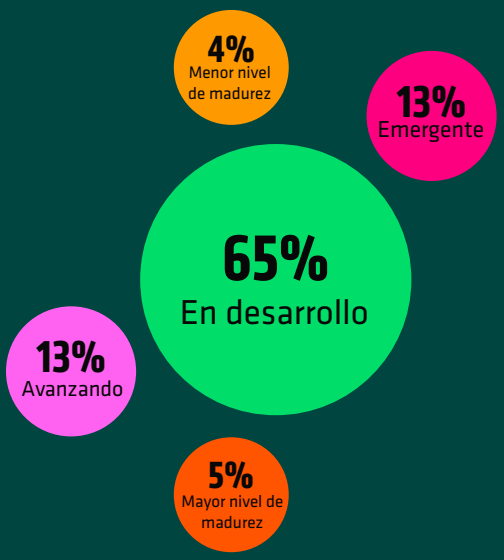
Identificar y priorizar los sistemas para los respaldos

Las organizaciones de servicios financieros están utilizando el descubrimiento y la clasificación de datos de manera más estratégica en los ámbitos del cumplimiento normativo, la respuesta y la recuperación. Alrededor de dos tercios abordan las violaciones de privacidad y seguridad, y utilizan la clasificación para orientar el cumplimiento durante un ataque; mientras que menos organizaciones definen la materialidad antes de un incidente o prioriza las copias de seguridad en función del riesgo. Estas brechas sugieren que el uso de la clasificación basado en el riesgo aún está evolucionando. Una ciberresiliencia madura transforma la clasificación en un enfoque sistemático que optimiza la postura ante el riesgo de los datos y proporciona información para la protección, la respuesta y la recuperación.

UNA IMAGEN MÁS CLARA DE LA MADUREZ DE LA RESILIENCIA

Al evaluarse de manera colectiva, las respuestas de los encuestados sirvieron como un barómetro de alto nivel de la madurez en ciberresiliencia, revelando patrones claros sobre cómo las organizaciones de servicios financieros están construyendo, o luchando por construir, dicha resiliencia en la práctica. Si bien la mayoría se encuentra en la etapa de desarrollo, solo el 5% demuestra las capacidades integradas más maduras que definen a las organizaciones preparadas para afrontar riesgos.

A CURVA DE MATURIDADE DA RESILIÊNCIA CIBERNÉTICA



Menor nivel de madurez (4%): Las respaldo, las políticas y las salvaguardas de seguridad están, en gran medida, ausentes o son inconsistentes. La autenticación multifactor y los controles administrativos rara vez se aplican, la recuperación a menudo carece de aislamiento y las evaluaciones de cumplimiento o materialidad suelen pasarse por alto.

Emergente (13%): Se han implementado algunas prácticas de resiliencia, pero de manera inconsistente. Las organizaciones pueden realizar respaldos de datos confidenciales, aplicar políticas globales o utilizar la MFA, pero rara vez de forma combinada. La inteligencia de amenazas y los esfuerzos de cumplimiento existen, pero siguen siendo inmaduros y fragmentados.

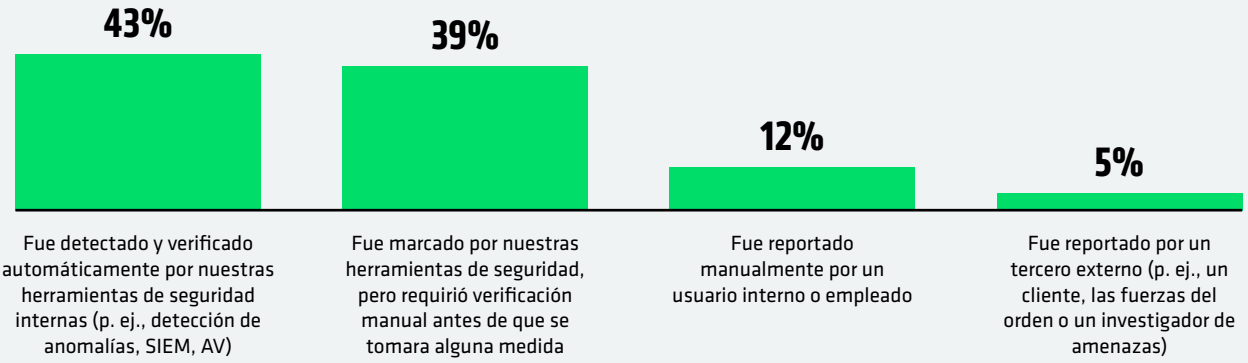
En desarrollo (65%): Las prácticas fundamentales, tales como los respaldos, los controles administrativos y la inteligencia sobre amenazas, son más comunes, aunque siguen siendo desiguales. Los entornos de recuperación, las verificaciones de cumplimiento y la remediación de brechas de seguridad se aplican de manera esporádica, lo que deja los esfuerzos de resiliencia con una eficacia parcial.

Avanzando (13%): La mayoría de las prácticas clave se aplican de manera sistemática, incluidas las políticas globales de respaldo, las aprobaciones administrativas y la remediación previa a la recuperación. La inteligencia de amenazas se utiliza, pero no está plenamente optimizada, y persisten algunas brechas en torno a la recuperación aislada y la cobertura total del cumplimiento normativo.

Mayor nivel de madurez (5%): La resiliencia es sistemática e integral. Los datos confidenciales se respaldan a nivel global, la MFA y los controles administrativos son estándar, la inteligencia de amenazas se maximiza, la recuperación se asegura mediante la remediación y las salvaguardas de cumplimiento se cumplen de manera constante.

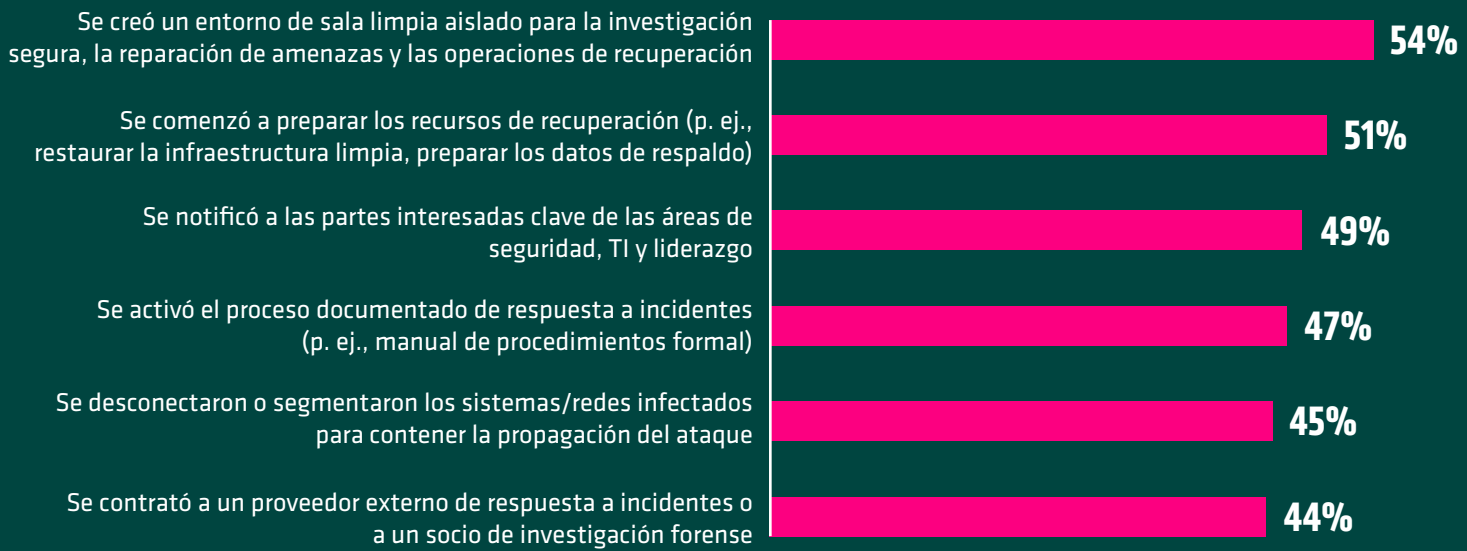
RESILIENCIA BAJO FUEGO

CÓMO LOS EQUIPOS IDENTIFICARON EL ATAQUE



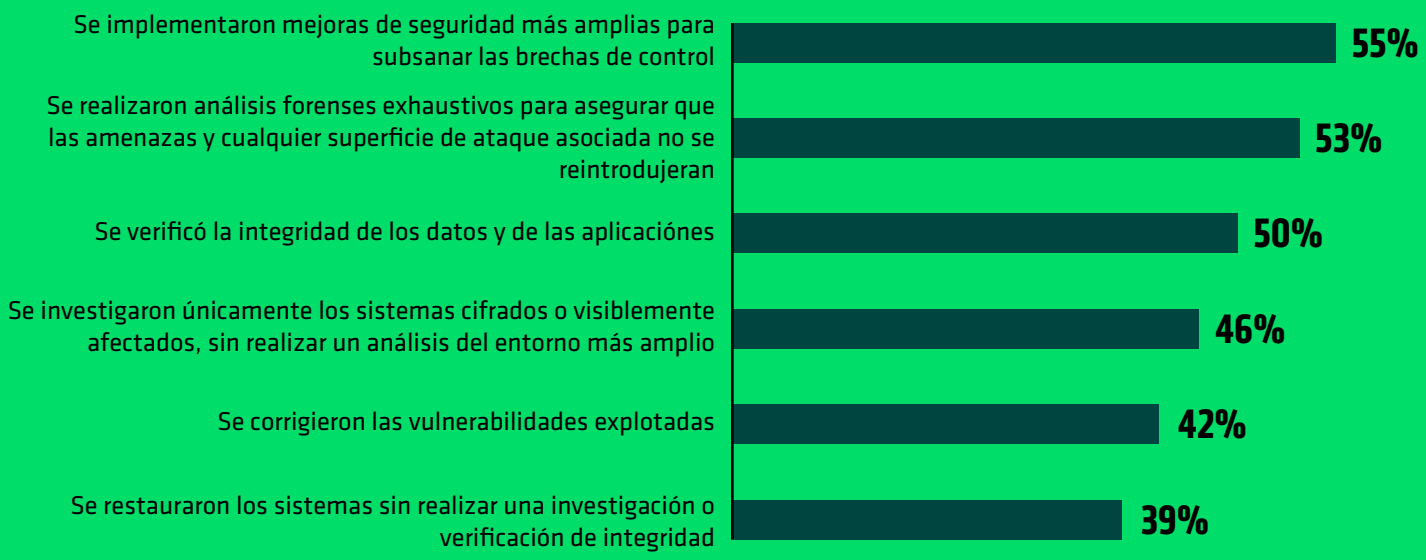
En caso de un ciberataque, la mayoría de las organizaciones de servicios financieros detectan los incidentes internamente. Casi la mitad afirmó que los ataques fueron identificados y verificados automáticamente por sus propias herramientas de seguridad, mientras que una proporción ligeramente menor indicó que los ataques fueron señalados por las herramientas, pero requirieron una verificación manual antes de tomar medidas. Solo una pequeña fracción fue identificada por terceros, lo que indica que la detección es en gran medida interna, pero sigue dependiendo de la confirmación humana.

ACCIONES QUE TOMARON LOS EQUIPOS TRAS CONFIRMAR EL ATAQUE



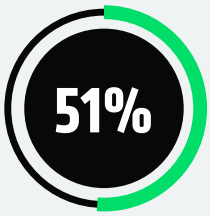
Tras confirmar un ataque, las organizaciones de servicios financieros adoptaron una serie de medidas para apoyar la recuperación. Poco más de la mitad comenzó a restaurar la infraestructura limpia o a preparar datos de respaldo, mientras que un porcentaje ligeramente mayor estableció entornos aislados de sala limpia para una investigación y recuperación seguras. Una proporción menor notificó a las partes interesadas clave, contuvo los sistemas infectados, activó manuales de respuesta formales o recurrió a expertos externos en respuesta a incidentes o en informática forense. Estas variaciones indican que las acciones de respuesta aún no están plenamente estandarizadas en los pasos críticos.

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

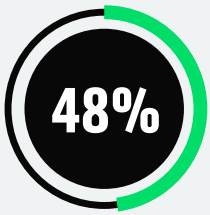


Antes de volver a poner los sistemas en línea, las organizaciones de servicios financieros llevaron a cabo una combinación de acciones forenses y de remediación. Más de la mitad implementó mejoras de seguridad más amplias o realizó análisis forenses completos. La mitad también verificó la integridad de los datos y de las aplicaciones, mientras que un número menor investigó más allá de los sistemas visiblemente afectados o aplicó parches a las vulnerabilidades explotadas. Más de un tercio restauró los sistemas sin una investigación exhaustiva ni verificación de la integridad, dejando brechas para la reinfección y un riesgo residual.

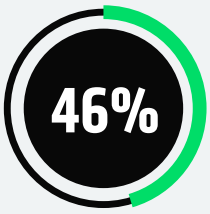
DESAFÍOS QUE ENFRENTARON LOS EQUIPOS DURANTE EL ATAQUE



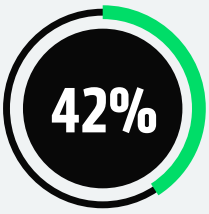
Incapacidad para comunicarse o coordinarse dentro de nuestro equipo debido a la caída de sistemas críticos (p. ej., correo electrónico, aplicaciones colaborativas, sistemas de gestión de incidencias)



Presión por parte de la dirección para restablecer los sistemas antes de que se remediara el ataque



Se eludieron las herramientas de seguridad y se atacaron los respaldos



Nos recuperamos, pero posteriormente nos reinfectamos porque las amenazas no fueron erradicadas por completo

Falta de acceso a puntos de recuperación limpios y validados

Los equipos reportaron dificultades significativas a lo largo del proceso. Muchos tuvieron dificultades para comunicarse o coordinarse mientras los sistemas críticos estaban fuera de servicio. Casi la mitad se vio presionada para restablecer las operaciones antes de que se completaran las labores de remediación. La evasión de las herramientas de seguridad, la reinfección y la falta de puntos de recuperación limpios agravaron las dificultades, lo que puso de manifiesto la necesidad de medidas de resiliencia más sólidas.

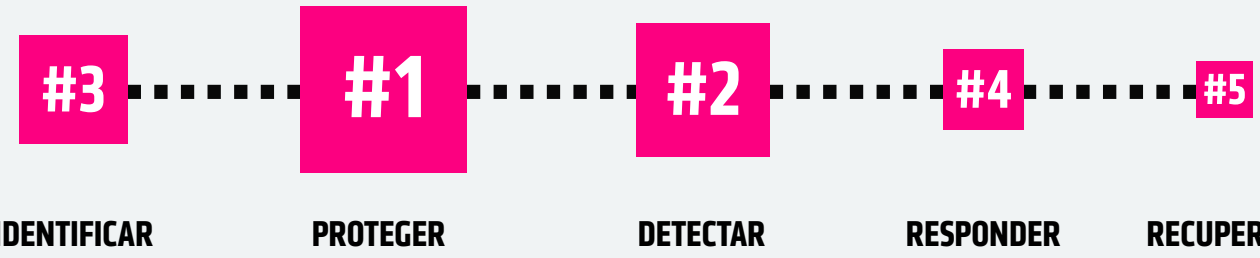
DÓNDE LA INVERSIÓN EN RESILIENCIA AÚN SE QUEDA CORTA

Incluso las organizaciones de servicios financieros mejor preparadas tienen dificultades para mantener la resiliencia una vez que se desata un ataque. A medida que aumenta la presión operativa, las brechas de coordinación, la remediación incompleta y los riesgos de reinfección ponen de manifiesto cuán frágil puede resultar la recuperación sin procesos unificados y una garantía continua.

Estos patrones reflejan la forma en que las organizaciones de servicios financieros están asignando sus presupuestos de ciberresiliencia en la actualidad. Preguntamos a los encuestados cómo distribuyen sus gastos entre las cinco funciones principales del Marco de Ciberseguridad del NIST: Identificar, Proteger, Detectar, Responder y Recuperar. La mayoría sigue invirtiendo fuertemente en prevención, protección y detección, mientras que se destinan comparativamente menos fondos a la respuesta y la recuperación verificada. El resultado es una curva de madurez que sigue inclinándose más hacia la defensa que hacia la restauración, lo que pone de manifiesto una oportunidad sin explotar para fortalecer la resiliencia donde más importa: después del ataque.

MARCO DE CIBERSEGURIDAD DEL NIST

El tamaño de la caja muestra la proporción más alta a la más baja de las inversiones en ciber-resiliencia



LA IA Y LA AUTOMATIZACIÓN EMERGEN COMO MULTIPLICADORES DE LA RESILIENCIA

Los resultados también muestran que las organizaciones de servicios financieros perciben la IA como un potente facilitador de la ciberresiliencia, particularmente en la mejora de 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 impulsada por IA como eficaces para fortalecer su postura de seguridad.

Incluso los asistentes más recientes basados en IA generativa, capaces de realizar consultas sobre amenazas mediante lenguaje natural y análisis contextual, están ganando terreno como medio para simplificar y acelerar la toma de decisiones. El 56% de las organizaciones de servicios financieros afirmó que una de las mayores lecciones aprendidas tras un ciberataque fue 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, coherencia y eficacia en estos procesos.

De cara al futuro, la mayoría prevé que la IA desempeñará un papel cada vez más estratégico en la ciberdefensa para finales de 2026. El 49% prevé que la IA respaldará la toma de decisiones humana, mejorando el análisis y las recomendaciones, mientras que los seres humanos mantendrán el control de las acciones finales. El 39% espera que la IA se convierta en un elemento central de la detección y la respuesta, llegando incluso a tomar algunas decisiones autónomas. Esto indica una trayectoria clara: La IA está evolucionando de ser un asistente a convertirse en una piedra angular operativa de la ciberresiliencia, 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 de servicios financieros están logrando avances mensurables en materia de ciberresiliencia, muchas aún tienen margen para mejorar su respuesta, recuperación y validación de la preparación tras un ataque. La ciberresiliencia 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 de los clientes y mantener la actividad empresarial cuando otras no pueden hacerlo. Cuando la disrupción es prácticamente inevitable, la resiliencia no es solo protección; es desempeño.

Desarrolle resiliencia antes de que estalle la crisis.

- Reserve un Taller sobre Resiliencia ante el Ransomware.
- Mejore su nivel con un plan de acción de cinco pasos para la ciberresiliencia.
- Conozca las Soluciones de Ciberresiliencia de Cohesity para el Sector de Servicios Financieros.

METODOLOGÍA

Cohesity encargó a Vanson Bourne la realización de una encuesta a 3,200 responsables de la toma de decisiones en TI y seguridad en septiembre de 2025, lo cual constituye la base de estos hallazgos. Los encuestados representan a organizaciones de EE.UU. (500), Brasil (200), Reino Unido (400), Alemania (400), Francia (400), Emiratos Árabes Unidos/Arabia Saudita (100), Australia (200), Corea del Sur (200), Japón (400), India (200) y Singapur (200). Las organizaciones contaban con 1,000 o más empleados y provenían de una variedad de sectores públicos y privados, con un enfoque en servicios financieros, el sector público y la atención médica.

COHESITY

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

2000082-001-ES 5-2026