COHESITY

INFORME DE CIBERRESILIENCIA

Preparados para el Riesgo o Expuestos al Riesgo: La Brecha de Ciberresiliencia en el Sector Público

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 el porqué 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 399 participantes de organizaciones del sector público. Sus respuestas revelan una creciente brecha en la capacidad de adaptación entre las organizaciones preparadas para afrontar riesgos, que pueden recuperarse con rapidez y confianza, y sus pares expuestas a riesgos, que siguen siendo vulnerables a interrupciones prolongadas y daños financieros posteriores.

Nuestra investigación examina los impactos reales de los ciberataques significativos, cómo las organizaciones del sector público autoevaluaron su resiliencia cibernética en comparación con las mejores prácticas y las medidas que tomaron para detectar, responder y recuperarse de estos incidentes. 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 gestionan intentos de phishing, sondeos de malware o interrupciones del sistema de forma casi diaria. Pero los ciberataques contra materiales son diferentes. Nuestra encuesta definió un ciberataque significativo como un incidente que causó un impacto cuantificable en las finanzas, la reputación, las operaciones o la pérdida de clientes.

ESTOS ATAQUES DE ALTO IMPACTO YA NO SON SUCESOS AISLADOS PARA LAS ORGANIZACIONES DEL SECTOR PÚBLICO.

67 %

de los encuestados ha sufrido al menos un ciberataque importante

49 %

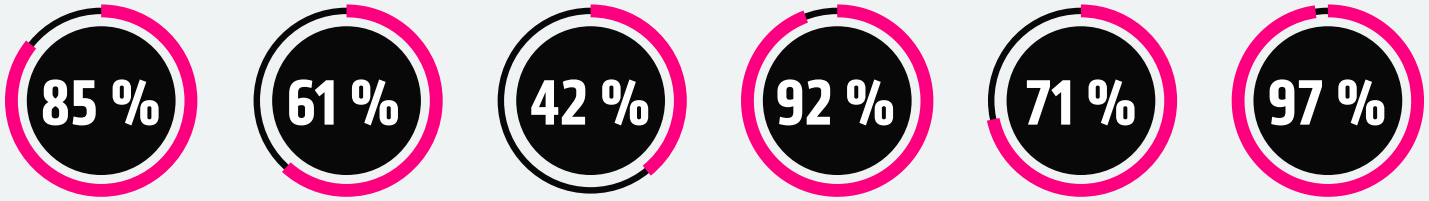
experimentó uno en los últimos 12 meses

26 %

sufrió múltiples incidentes durante el período de 12 meses

EL COSTE REAL DE LOS CIBERATAQUES MATERIALES

LAS PRESIONES FINANCIERAS Y REGULATORIAS SE HICIERON ECO EN TODAS LAS ORGANIZACIONES DEL SECTOR PÚBLICO QUE ENCUESTAMOS:



reportó pérdidas de ingresos

de las organizaciones que cotizan en bolsa informaron 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 (45 %) y demandas o litigios colectivos (40 %)

[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

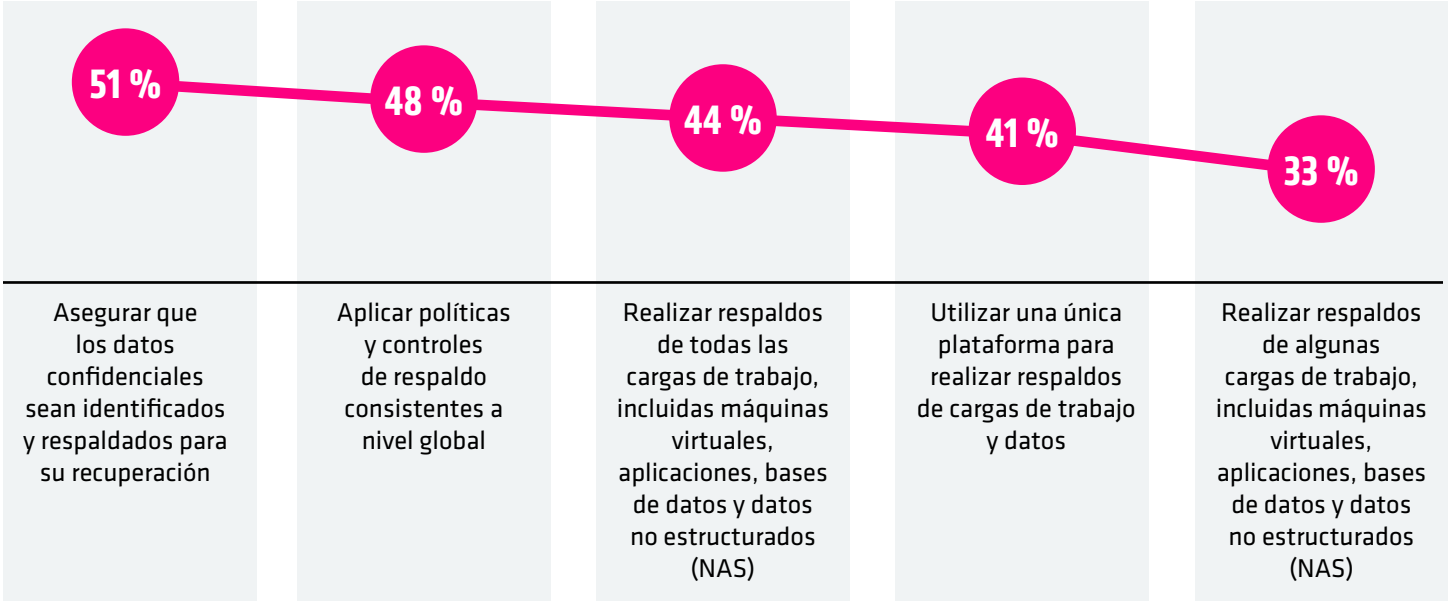
Dada la magnitud de las consecuencias financieras y operativas reveladas en nuestra investigación, cabría esperar una preocupación generalizada por la resiliencia de las organizaciones. Sin embargo, la mayoría de los encuestados (54 %) expresó plena confianza en que su estrategia de ciberresiliencia 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?



Poco más de la mitad de las organizaciones del sector público se aseguran de que los datos confidenciales se identifiquen y se respalden para su recuperación, mientras que cerca de la mitad aplican políticas y controles de respaldo uniformes a nivel mundial. Menos de la mitad realiza respaldos de todas las cargas de trabajo o utiliza una única plataforma para proteger las cargas de trabajo y los datos. Un tercer respaldo 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.

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

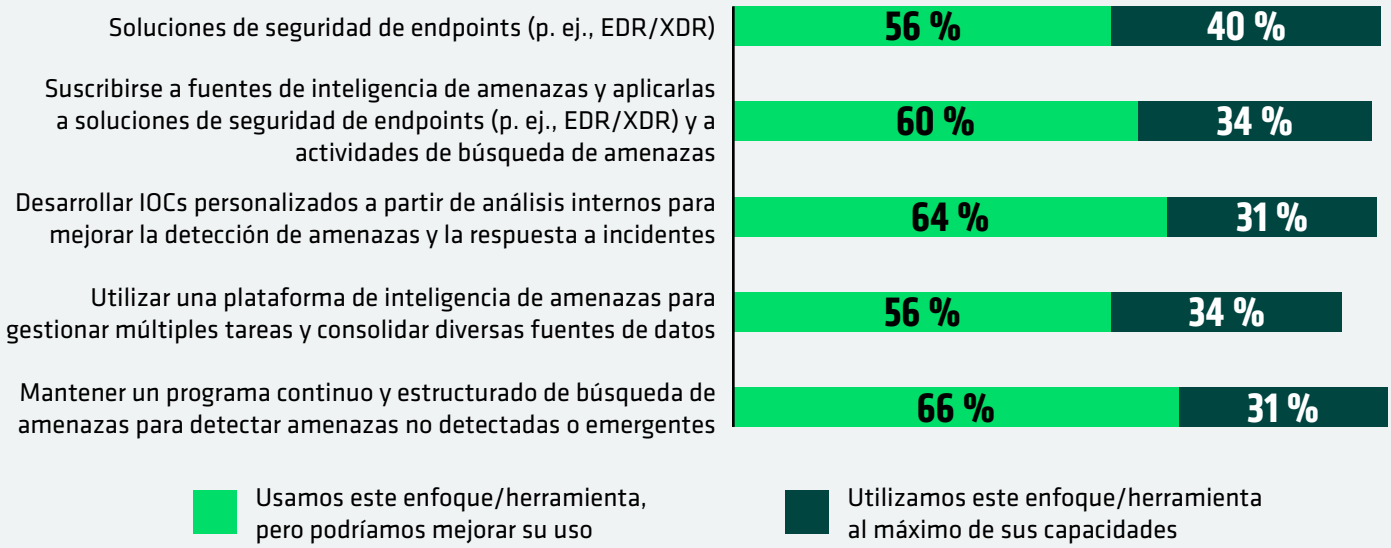
¿Qué hace su organización para garantizar que sus datos sean siempre recuperables?

50 %	Exigir autorización adicional para las tareas administrativas de alto riesgo asociadas a las soluciones de respaldo y recuperación
47 %	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)
46 %	Autenticación multifactor en su solución de respaldo
46 %	Aplicar principios de acceso de privilegio mínimo en las cargas de trabajo respaldadas
38 %	Proteger los datos críticos con inmutabilidad

Muchas organizaciones del sector público han reforzado los controles de acceso a los entornos de copia de seguridad, y la mitad de ellas exigen autorización administrativa adicional para tareas de alto riesgo. Aproximadamente la mitad implementan la autenticación multifactor, siguen la regla de respaldo 3-2-1 y aplican derechos de acceso con privilegios mínimos. Son pocos los que protegen los datos críticos con inmutabilidad. 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 del sector público utilizan seguridad de endpoints, fuentes de inteligencia sobre amenazas, indicadores de compromiso (IOC) personalizados, plataformas de inteligencia sobre amenazas y programas estructurados de búsqueda de amenazas; sin embargo, solo una minoría aprovecha al máximo estas herramientas. 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?

57 % 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

52 % Utilizar un entorno aislado para la investigación de incidentes, la remediación y la recuperación segura

48 % Identificar y subsanar las brechas en los controles de seguridad antes de restaurar los sistemas a producción

43 % Mantener un repositorio en línea y seguro de sistemas críticos e información para respaldar la respuesta a incidentes y la recuperación

36 % Aplicar inmutabilidad para todos los datos de respaldo

Las organizaciones del sector público están mejorando su enfoque para lograr una mayor resiliencia de las aplicaciones, pero aún existen deficiencias. Casi la mitad identifica fallos en los controles de seguridad antes de restaurar los sistemas, y más de la mitad realiza simulacros de recuperación anuales. Un poco más de la mitad mantienen repositorios en línea protegidos mediante bóvedas, mientras que un número menor utiliza entornos aislados para la investigación y recuperación seguras. Un porcentaje aún menor 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 ESTÁ GANANDO TERRENO, PERO SU USO BASADO EN EL RIESGO AÚN ESTÁ EN EVOLUCIÓN

¿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?

58 %

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

57 %

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

53 %

Identificar y priorizar los sistemas para los respaldos

51 %

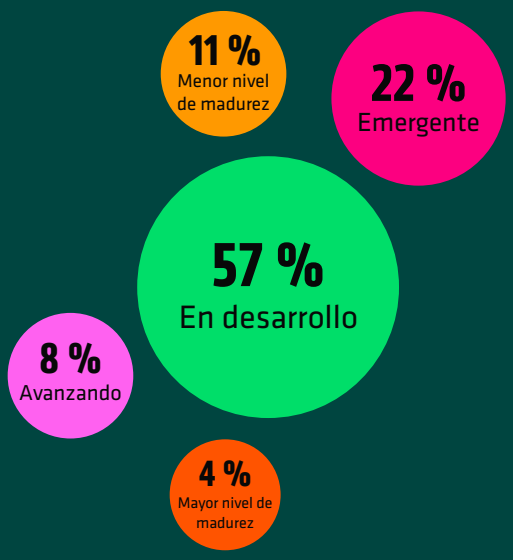
Definir y comprender la materialidad de los ciberataques antes de que ocurra un incidente

Las organizaciones del sector público están utilizando el descubrimiento y la clasificación de datos de forma más estratégica en materia de cumplimiento normativo, respuesta y recuperación. Más de la mitad abordan las violaciones de privacidad y seguridad, mientras que poco más de la mitad utilizan la clasificación para orientar el cumplimiento durante un ataque y definir la materialidad antes de un incidente. Una proporción similar prioriza los respaldos en función del riesgo. Estos patrones sugieren que el uso de la clasificación en función del riesgo aún está en evolución. 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

En conjunto, las respuestas de los encuestados sirvieron como un barómetro de alto nivel sobre la madurez de la ciberresiliencia, revelando patrones claros sobre cómo las organizaciones del sector público están construyendo, o luchando por construir, la resiliencia en la práctica. Si bien la mayoría se encuentra en la etapa de desarrollo, solo el 4 % 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 (11 %): Los respaldos, 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 (22 %): 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.

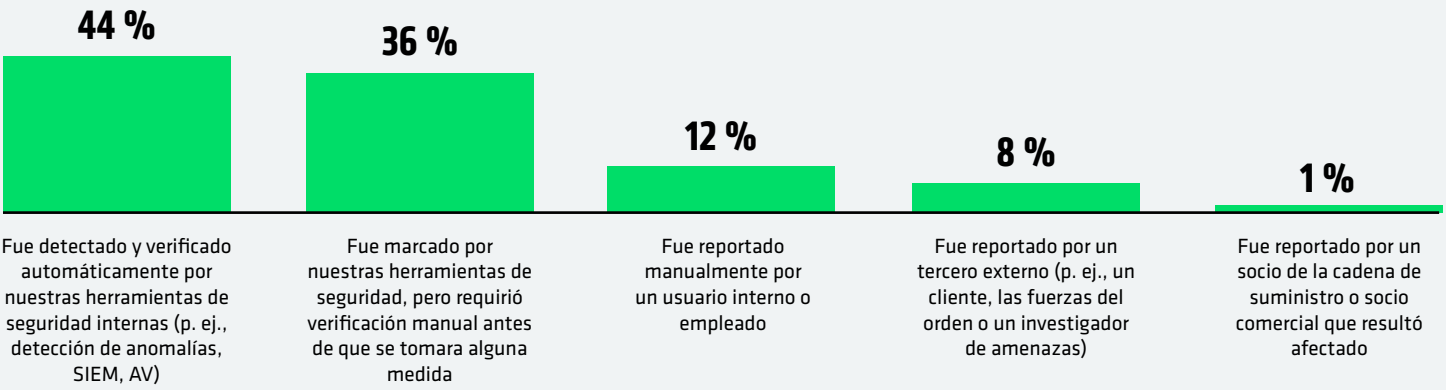
En desarrollo (57 %): Las prácticas fundamentales, tales como los respaldos, los controles administrativos y la inteligencia sobre amenazas, son más comunes, aunque siguen siendo desiguales. Los entornos de recuperación, las verificaciones de cumplimiento y la remediación de brechas de seguridad se aplican de manera esporádica, lo que deja los esfuerzos de resiliencia con una eficacia parcial.

Avanzando (8 %): 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 (4 %): 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.

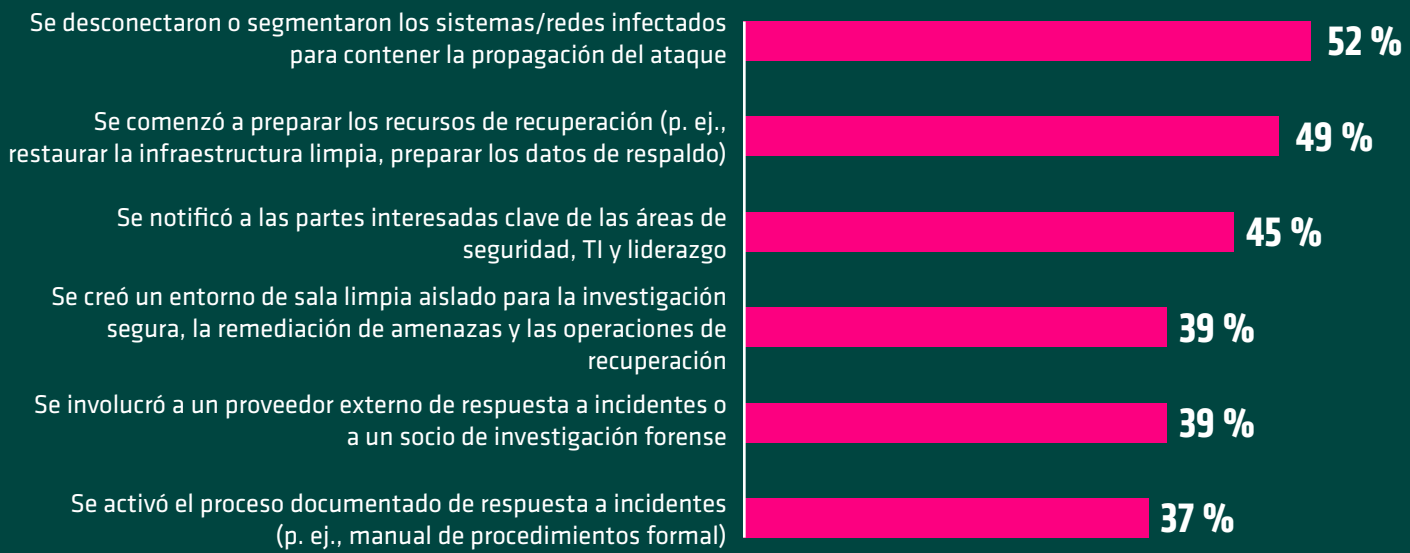
RESILIENCIA BAJO FUEGO

CÓMO LOS EQUIPOS IDENTIFICARON EL ATAQUE



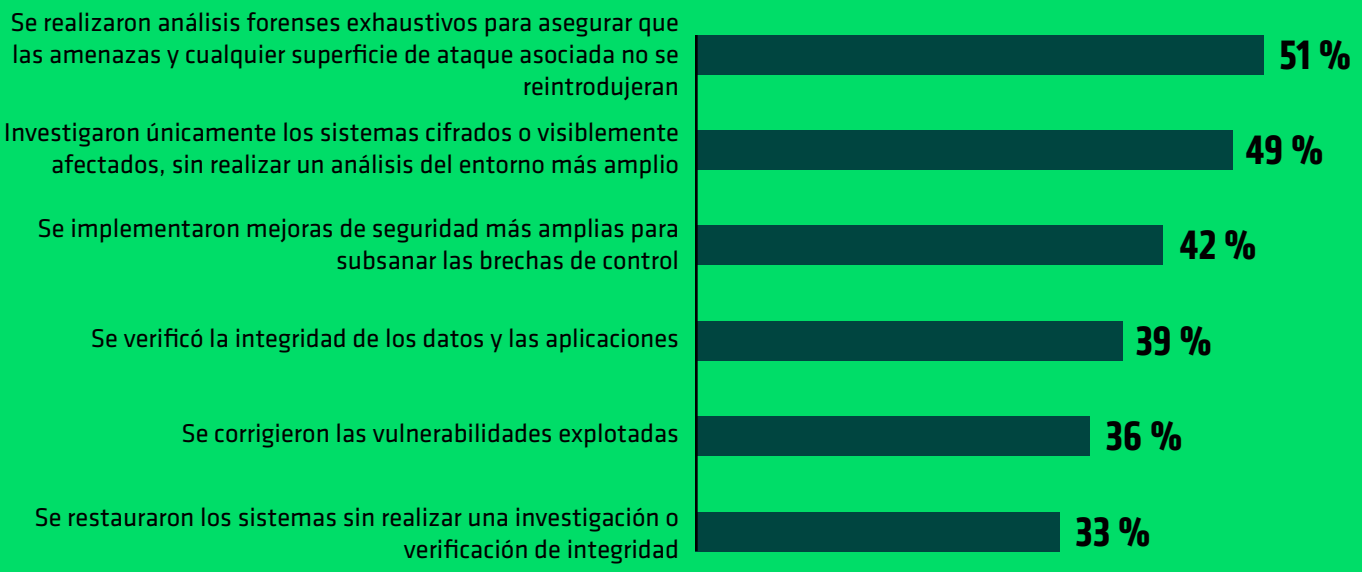
En caso de un ciberataque, la mayoría de las organizaciones del sector público detectan los incidentes internamente. La mayor parte son identificadas y verificadas automáticamente por herramientas de seguridad, mientras que muchas otras son señaladas por herramientas pero requieren verificación manual. Los empleados o terceros denuncian muchos menos incidentes. La detección se basa en gran medida en herramientas, aunque la validación humana sigue desempeñando un papel importante.

MEDIDAS ADOPTADAS POR LOS EQUIPOS TRAS CONFIRMAR EL ATAQUE



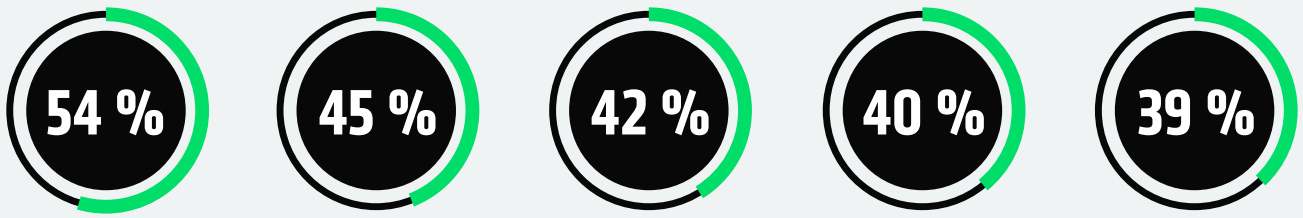
Tras confirmar el ataque, las organizaciones del sector público adoptaron diversas medidas para contener la amenaza e iniciar la recuperación. Aproximadamente la mitad desconectaron los sistemas infectados o comenzaron a preparar recursos para la recuperación, mientras que muchos notificaron a las partes interesadas clave. Las participaciones más pequeñas crearon entornos de sala limpia aislados, activaron planes de respuesta formales o involucraron a socios externos de respuesta a incidentes. Estas diferencias sugieren que los esfuerzos de respuesta aún no están estandarizados de manera consistente en todas las acciones críticas.

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



Antes de restablecer los sistemas y los datos, las organizaciones del sector público adoptaron una serie de medidas forenses y de remediación. Aproximadamente la mitad realizó un análisis forense completo o se centró únicamente en los sistemas visiblemente afectados, mientras que un número menor implementó mejoras de seguridad más amplias, verificó la integridad o corrigió las vulnerabilidades explotadas. Cabe destacar que aproximadamente un tercio de los sistemas se restauraron sin investigación ni verificación, lo que deja posibles lagunas que podrían aumentar el riesgo de reinfección o exposición 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

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

Se eludieron las herramientas de seguridad y se atacaron los respaldos

Falta de acceso a puntos de recuperación limpios y validados

Los equipos se enfrentaron a importantes desafíos operativos y técnicos durante el ataque. Muchos tuvieron dificultades para comunicarse mientras los sistemas críticos estaban fuera de servicio y sintieron la presión de restablecer los sistemas antes de que se completara la solución del problema. Otros informaron de la evasión de las herramientas de seguridad, ataques a los respaldos, falta de puntos de recuperación limpios o incluso reinfección después de la recuperación. Estas dificultades ponen de manifiesto deficiencias en la preparación que pueden complicar la respuesta y prolongar las interrupciones.

DONDE LA INVERSIÓN EN RESILIENCIA AÚN SE QUEDA CORTA

Incluso las organizaciones mejor preparadas tienen dificultades para mantener la capacidad de respuesta una vez que se produce un ataque. A medida que aumenta la presión operativa, las deficiencias en la coordinación, la remediación incompleta y los riesgos de reinfección ponen de manifiesto la fragilidad de la recuperación sin procesos unificados y una garantía continua.

Estos patrones reflejan la forma en que las organizaciones del sector público están asignando sus presupuestos de ciberseguridad en la actualidad. 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 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 del sector público consideran la IA como un poderoso facilitador de la ciberresiliencia, en particular para mejorar la velocidad de detección y la precisión de la respuesta. Casi todos los encuestados consideraron que herramientas como la detección de anomalías, el análisis del comportamiento del usuario y la investigación y respuesta ante amenazas basadas en inteligencia artificial son eficaces para fortalecer su postura de seguridad.

Incluso los asistentes más recientes 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 del sector público 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 todos 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 43 % prevé que la IA respaldará la toma de decisiones humanas, mejorando el análisis y las recomendaciones, aunque los humanos seguirán teniendo el control de las acciones finales. El 42 % 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 del sector público están logrando avances significativos en materia de ciberresiliencia, muchas aún tienen margen de mejora en 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 del cliente y seguir adelante con el negocio cuando otros no pueden. Cuando la disrupción es prácticamente inevitable, la resiliencia no es solo protección; es rendimiento.

Desarrolle resiliencia antes de que llegue 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 ciberseguridad de Cohesity para el Sector Público.
  - Gobierno federal
  - Gobierno estatal, local y educación

METODOLOGÍA

COHESITY

Cohesity encargó a Vanson Bourne que realizara una encuesta a 3,200 responsables de la toma de decisiones en materia de TI y seguridad en septiembre de 2025, lo que sirvió de base para estas conclusiones. 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 pertenecían a diversos sectores públicos y privados, con especial atención a los servicios financieros, el sector público y la sanidad.

COHESITY

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

2000089-001-ES 6-2026