INFORME

El estado del ransomware 2026

Reflexiones de 2158 responsables de TI y ciberseguridad de 17 países

SOPHOS

Introducción

El panorama del ransomware está cambiando rápidamente a raíz del avance de la IA. Es evidente que las organizaciones que realizan inversiones sostenidas en defensas de ciberseguridad obtienen mejores resultados, pero los ataques de ransomware siguen costando millones a las empresas.

Esta es la séptima edición del informe anual de Sophos sobre el estado del ransomware, que ofrece nuevos datos sobre los ataques de ransomware del último año. Las conclusiones se recogen en secciones que abarcan:

- Los métodos de ataque y defensa
- El cifrado y la recuperación de datos
- El importe del rescate exigido y el importe abonado
- El impacto a nivel empresarial y humano

Los datos reflejan una situación en la que los resultados costosos se entremezclan con avances reales:

- Los costes de recuperación tras un ataque de ransomware son elevados; actualmente, el coste medio de la recuperación asciende a 1,7 millones USD.
- Más de la mitad de los ataques de ransomware (56 %) siguen logrando cifrar los datos, y el índice aumentará a partir de 2025.
- Sin embargo, el importe del rescate exigido y el importe abonado están disminuyendo, y las organizaciones cada vez se desenvuelven mejor a la hora de negociar los resultados. En los últimos dos años, la mediana de las peticiones ha descendido un 65 % y los pagos se han reducido un 62 %.
- Tras tres años ocupando el primer puesto, la explotación de vulnerabilidades ya no es la principal causa raíz de los ataques de ransomware (18 %); ahora, los ataques a través del correo electrónico (phishing, 24 %, o correos electrónicos maliciosos, 26 %) son los vectores de ataque más habituales.

2158

responsables de TI y seguridad de 17 países, cuyas organizaciones se vieron afectadas por un ataque de ransomware durante el último año, participaron en una encuesta global independiente del proveedor, que ha servido de base para el estudio de este año.

Acerca de la encuesta

Este informe se basa en los resultados de una encuesta independiente y desvinculada del proveedor encargada por Sophos. La encuesta se centró en la experiencia de las organizaciones ante los ataques de ransomware y las intrusiones basadas en la identidad, realizando un seguimiento año tras año de los índices de pago del rescate, los costes de restauración, los plazos de recuperación y muchos otros indicadores. Las respuestas se recabaron entre enero y marzo de 2026 y se basan en las experiencias de los encuestados durante los 12 meses anteriores.

Los participantes procedían de 17 países y de una amplia variedad de sectores, tanto del ámbito público como del privado, y la distribución de las organizaciones (con un número de empleados comprendido entre 100 y 5000) se ha mantenido proporcionalmente constante a lo largo de los siete años de historia de la encuesta. Todos los puntos de datos financieros son en dólares estadounidenses (USD).

Conclusiones clave de un vistazo

- **El robo de identidad es el principal mecanismo de distribución del ransomware**
  - Los correos electrónicos maliciosos (26 %) y el phishing (24 %) se han convertido en las principales causas raíz de los ataques de ransomware.
  - La explotación de vulnerabilidades, la causa raíz más importante de los últimos tres años, se ha reducido en 14 puntos porcentuales con respecto al año pasado, hasta situarse en el 18 %.
  - Dos tercios de las víctimas de ransomware (el 67 %) confirmaron que su incidente de ransomware fue también el ataque más grave relacionado con la identidad.
- **Las deficiencias en materia de protección, seguridad y recursos dejan a las organizaciones expuestas a los ataques**
  - Por segundo año consecutivo, las lagunas de seguridad (conocidas o desconocidas) fueron las causas raíz operativas más citadas, con un 62 %, seguidas de la falta de personal o de conocimientos (58 %) y la falta de protección o la protección deficiente (57 %).
- **El despliegue de la autenticación multifactor (MFA) por sí sola no basta para detener el ransomware**
  - La MFA estaba presente, en mayor o menor medida, en el 97 % de los incidentes en los que el compromiso de credenciales fue la causa raíz de los ataques de ransomware.
- **En más de la mitad de los incidentes, las organizaciones no logran detectar ni detener a tiempo los ataques de ransomware**
  - Más de la mitad de los ataques de ransomware (56 %) lograron cifrar los datos, incluido un 16 % en los que los datos no solo se cifraron, sino que también se robaron.
- **Cuando los datos se cifran, los atacantes tienen aproximadamente un 50 % de probabilidades de recibir el pago del rescate**
  - El 48 % de las organizaciones cuyos datos fueron cifrados pagaron el rescate.
  - La media de los últimos cuatro años se sitúa ahora en un 50 % de los rescates pagados tras el cifrado.
- **Las peticiones de rescate están disminuyendo, pero los atacantes tienden a pedir más cuando logran vulnerar un sistema con privilegios cuyo acceso es difícil de restablecer**
  - La mediana de la cifra exigida en concepto de rescate descendió a 698 000 USD, lo que mantiene la tendencia a la baja observada desde hace varios años, partiendo de una mediana de 1,3 millones USD en el informe de 2025 y de 2 millones USD en el informe de 2024.
  - El 59 % de las peticiones de rescate derivadas de ataques que comenzaron con la explotación de una vulnerabilidad en el firewall ascienden a 1 millón USD o más, frente al 48 % del total de las peticiones.
- **Los importes de rescate abonados están disminuyendo, ya que las víctimas suelen conseguir negociar una cantidad inferior a la exigida inicialmente**
  - El importe medio de los rescates pagados asciende ahora a 769 000 USD, lo que supone un descenso considerable con respecto al millón USD registrado el año pasado.
  - Poco menos de la mitad (48 %) de los pagos fueron de 1 millón USD o más, una cifra inferior al 52 % del año anterior.
  - Casi la mitad (51 %) de las organizaciones que pagaron un rescate abonaron una cantidad inferior a la exigida, lo que coincide en gran medida con el informe de 2025 (53 %) y supone un aumento del 7 % con respecto al informe de 2024 (44 %).
- **El coste de recuperación tras un ataque de ransomware ha aumentado**
  - El coste medio de la recuperación tras un ataque de ransomware, sin tener en cuenta el rescate pagado, asciende actualmente a 1 700 200 USD, lo que supone un aumento del 11 % con respecto a la media de 1 525 716 USD del informe de 2025.
- **El cifrado de datos casi siempre tiene repercusiones para los miembros del equipo de TI/ciberseguridad**
  - El 99 % de las víctimas de ransomware cuyos datos fueron cifrados afirmaron que esto afectó a su equipo de TI/ciberseguridad.
  - El aumento de la ansiedad o el estrés ante posibles ataques futuros es la repercusión más habitual (41 %), seguida del aumento de la presión por parte de los altos cargos (40 %).
  - El mayor reconocimiento por parte de los altos directivos (un 36 %, frente al 31 % del informe de 2025) fue el único impacto que aumentó con respecto al año anterior.

Métodos de ataque y defensa

Causas raíz de los ataques

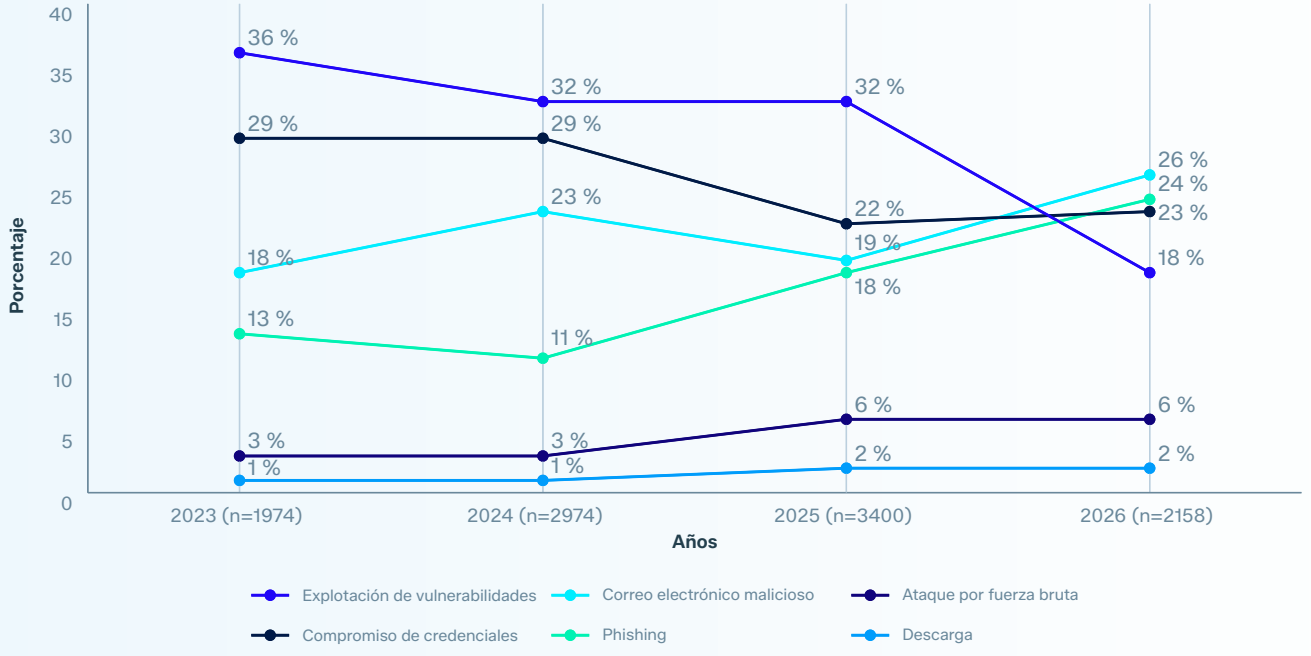
Las principales causas raíz técnicas del ransomware han cambiado en el informe de este año. Los correos electrónicos maliciosos (26 %) y el phishing (24 %) han sido las dos principales causas raíz de los ataques de ransomware, responsables de la mitad del total de incidentes. sto supone un cambio significativo con respecto a años anteriores, en los que la explotación de vulnerabilidades ocupaba sistemáticamente los primeros puestos de la clasificación.

El número de vulnerabilidades explotadas se ha reducido, pasando del 32 % en el informe de 2025 al 18 % en el de 2026. No obstante, dada la rapidez y el alcance de las capacidades de detección de vulnerabilidades que ofrece la IA de última generación, las organizaciones deben permanecer atentas a la posibilidad de que, durante el próximo año, se produzca un aumento de los ataques de ransomware cuya causa raíz sea la explotación de una vulnerabilidad.

El compromiso de credenciales ha permanecido como la tercera causa raíz más frecuente, con un 23 %, en línea con los años anteriores.

El 79 % de los ataques se iniciaron mediante un enfoque basado en la identidad, ya fuera para obtener credenciales con el fin de hacer un uso indebido de ellas o para explotar credenciales que ya se habían obtenido. Esto pone de relieve por qué la seguridad de la identidad es un elemento fundamental en una postura de seguridad integral.

Causa raíz técnica de los ataques de ransomware (2023-2026)



¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? Números base en la tabla.

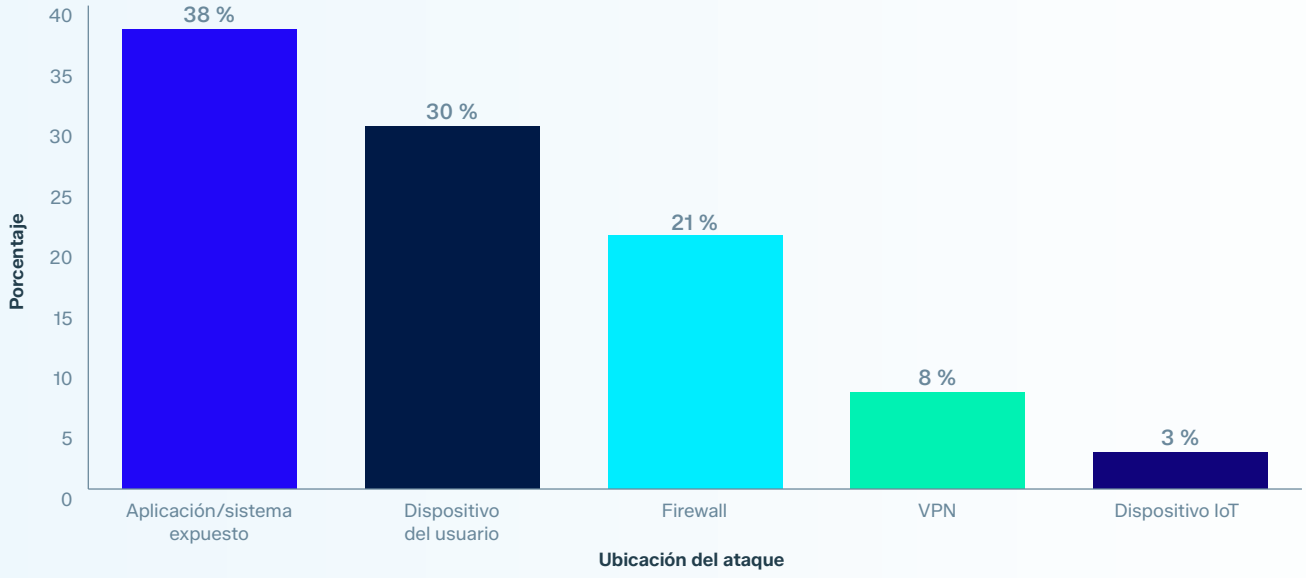
NUEVA INVESTIGACIÓN

Dónde se originan los ataques

Este año, por primera vez, revelamos dónde se sitúa la causa raíz dentro del entorno de la organización. Comprender dónde se originan los ataques es un elemento fundamental para diseñar estrategias de reducción de riesgos. Entre los incidentes de ransomware que se iniciaron a raíz de la explotación de una vulnerabilidad, el compromiso de credenciales o un ataque por fuerza bruta, **las aplicaciones y los sistemas expuestos constituyeron, en general, el punto de entrada más habitual (38 %)**, seguidos de los dispositivos de los usuarios (30 %) y los firewalls (21 %).

La mayor presencia de apps expuestas coincide con la tendencia generalizada hacia entornos en la nube y de SaaS, en los que los sistemas conectados a Internet presentan una superficie de ataque amplia y cada vez mayor.

Ubicaciones de los ataques de ransomware



Ha indicado que la causa raíz fue la explotación de vulnerabilidades, el compromiso de credenciales o un ataque por fuerza bruta. ¿En qué parte de su entorno ocurrió esto? n=1022

Al analizar los datos con mayor detalle, se observa la predominancia de credenciales vulneradas en apps y sistemas expuestos, firewalls, VPN y dispositivos del Internet de las cosas (IoT).

Causas raíz más frecuentes en cada ubicación

Causa raíz	En una aplicación o sistema expuesto	En nuestro firewall	En nuestra VPN	En un dispositivo IoT
Compromiso de credenciales	59 %	41 %	44 %	48 %
Explotación de vulnerabilidades	31 %	33 %	41 %	36 %
Ataque por fuerza bruta	10 %	26 %	15 %	16 %

Ha indicado que la causa raíz fue la explotación de vulnerabilidades, el compromiso de credenciales o un ataque por fuerza bruta. ¿En qué parte de su entorno ocurrió esto? Selección de respuestas. n=711

Los ataques de compromiso de credenciales fueron especialmente frecuentes en aplicaciones y sistemas expuestos (59 %), lo que refuerza la importancia de proteger los recursos accesibles desde el exterior y los controles de identidad.

Al volver a analizar la misma comparación de datos, se ponen de manifiesto los principales objetivos del compromiso de credenciales y de los ataques por fuerza bruta.

Dónde se originan los ataques de ransomware

Ubicación del ataque	% total	% compromiso de credenciales	% ataques por fuerza bruta
En una aplicación o sistema expuesto	38 %	46 %	30 %
En el dispositivo del usuario (conectado o no a la red, p. ej., ordenador portátil o de sobremesa).	30 %	27 %	13 %
En nuestro firewall	21 %	18 %	44 %
En nuestra VPN	8 %	7 %	9 %
En un dispositivo IoT	3 %	3 %	4 %

Ha indicado que la causa raíz fue el compromiso de credenciales o un ataque por fuerza bruta. ¿En qué parte de su entorno ocurrió esto? Selección de respuestas. n=628

Los distintos tipos de ataques se dirigieron a diferentes ubicaciones.

- Los ataques de compromiso de credenciales se centraron en apps y sistemas expuestos (46 %), seguidos de los dispositivos de los usuarios.
- Los ataques de fuerza bruta se dirigían principalmente a los firewalls (44 %), lo que pone de relieve la importancia de las políticas de limitación de frecuencia y de bloqueo de cuentas en los dispositivos periféricos de la red.

NUEVA INVESTIGACIÓN

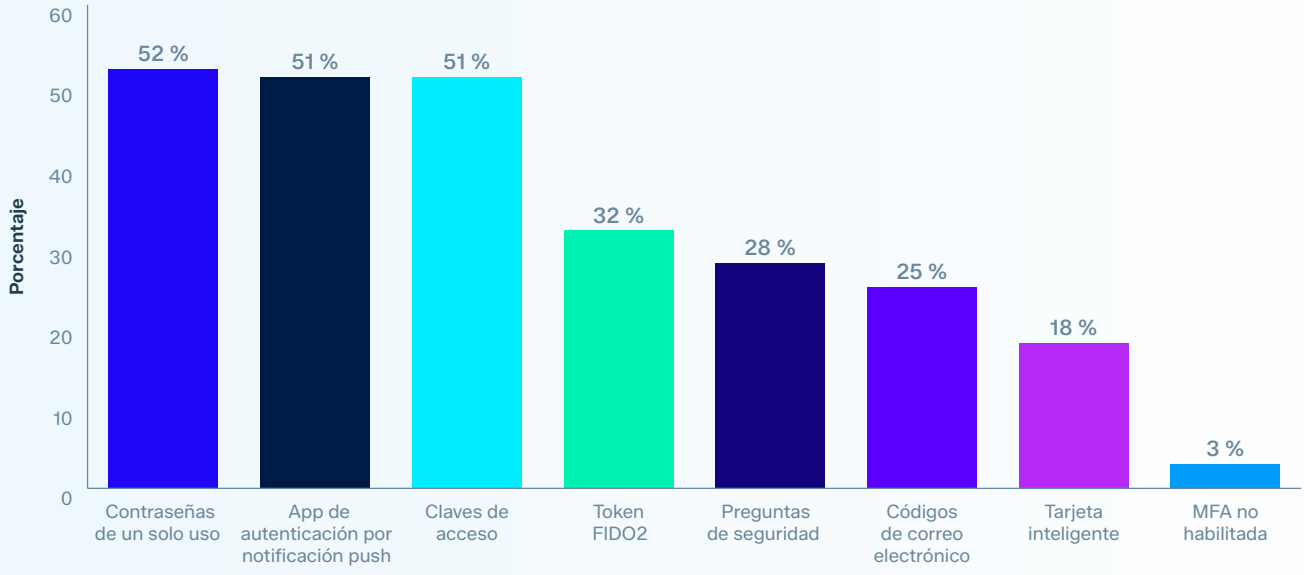
El papel de la autenticación multifactor (MFA)

Este año también se presentan nueva información sobre el papel de la MFA en los ataques de ransomware.

Entre las organizaciones en las que el compromiso de las credenciales fue la causa raíz del ataque de ransomware, **el 97 % tenía habilitada la autenticación multifactor de alguna forma en el momento del incidente**. Las contraseñas de un solo uso (52 %), las apps de autenticación por notificación push (51 %) y las claves de acceso (51 %) fueron los métodos más usados, y los encuestados indicaron que empleaban, de media, 2,5 métodos de autenticación multifactorial.

El elevado porcentaje de víctimas de ransomware que tenían implementado un método MFA en el momento del ataque indica que es posible que dicho método no se hubiera implementado por completo en todos los sistemas pertinentes, lo que creó brechas de seguridad que los atacantes pudieron explotar. También sugiere que, si bien la MFA sigue siendo un elemento esencial de las estrategias eficaces de ciberdefensa, no basta por sí sola para prevenir los ataques basados en credenciales, ya que las técnicas para eludirla siguen evolucionando.

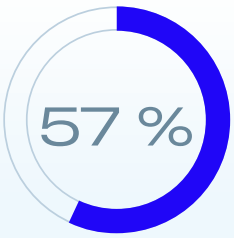
Métodos de MFA habilitados en el momento del ataque



¿Qué tipo de autenticación multifactor estaba habilitada en el momento del ataque, de ser el caso?
Base: El ataque se produjo debido al compromiso de credenciales. n=503

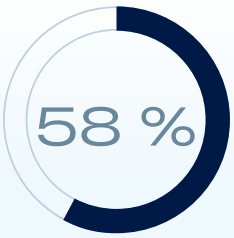
Factores de vulnerabilidad de las organizaciones

Por segundo año consecutivo, no se aprecia ningún factor organizativo concreto que haya expuesto a las organizaciones a los ataques: los encuestados han señalado una amplia variedad de dificultades, que van desde la falta de protección o una protección deficiente y la escasez de personal o de conocimientos, hasta las lagunas de seguridad.



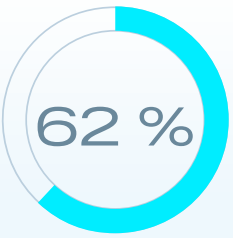
Problemas de protección

(falta de soluciones de protección o soluciones deficientes)



Problemas de recursos

(falta de conocimientos o de personal/ capacidad)



Laguna de seguridad

(conocida o desconocida)

Las deficiencias en materia de seguridad fueron la categoría más citada entre las causas raíz operativas por segundo año consecutivo, con un 62 %, seguidas de la falta de personal o de conocimientos (58 %) y la falta de protección o la protección deficiente (57 %).

Resulta alentador que todos los factores individuales (excepto uno) hayan registrado un descenso interanual, siendo **el error humano (35 %) el solo factor operativo que ha aumentado en el último año**.

Al igual que en 2025, las víctimas de ransomware señalaron múltiples retos organizativos, con **una media de 2,5 factores citados**, lo que supone un descenso respecto a los 2,7 anteriores.

35 %

El error humano: la sola constante. La única causa raíz operativa de los ataques que no se ha reducido con respecto al informe de 2025.

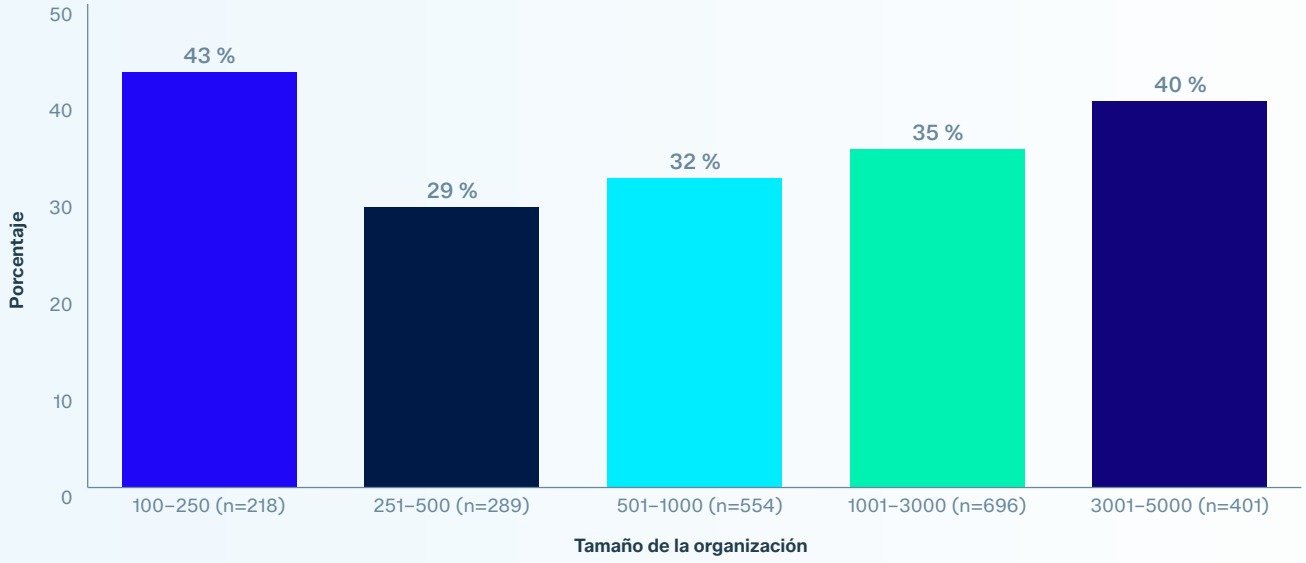
Las 7 principales causas raíz operativas de los ataques de ransomware

Puesto	2025	%	Puesto	2026	%
1	Falta de conocimientos especializados	40,2 %	1	Falta de protección	36,4 %
2	Laguna de seguridad desconocida	40,1 %	2	Laguna de seguridad desconocida	36,3 %
3	Falta de personal/ capacidad	39,4 %	3	Laguna de seguridad conocida	36,0 %
4	Falta de protección	39,0 %	4	Falta de personal/ capacidad	35,3 %
5	Laguna de seguridad conocida	38,2 %	5	Error humano	35,3 %
6	Protección deficiente	37,1 %	6	Falta de conocimientos especializados	35,1 %
7	Error humano	34,2 %	7	Protección deficiente	32,6 %

¿Por qué cree que su organización sufrió un ataque de ransomware? n=3400 (2025), n=2158 (2026)

Como era de esperar, la falta de personal/capacidad fue una de las principales dificultades mencionadas por las pequeñas organizaciones con un número de empleados comprendido entre 100 y 250. Sin embargo, cuatro de cada diez organizaciones con entre 3001 y 5000 empleados también mencionan dificultades de capacidad, con un índice que solo es un 3 % inferior al de las organizaciones con entre 100 y 250 empleados, lo que indica que la asignación de recursos no siempre resulta más sencilla a medida que aumenta el tamaño de la organización.

La falta de personal/capacidad contribuyó a sufrir un ataque de ransomware



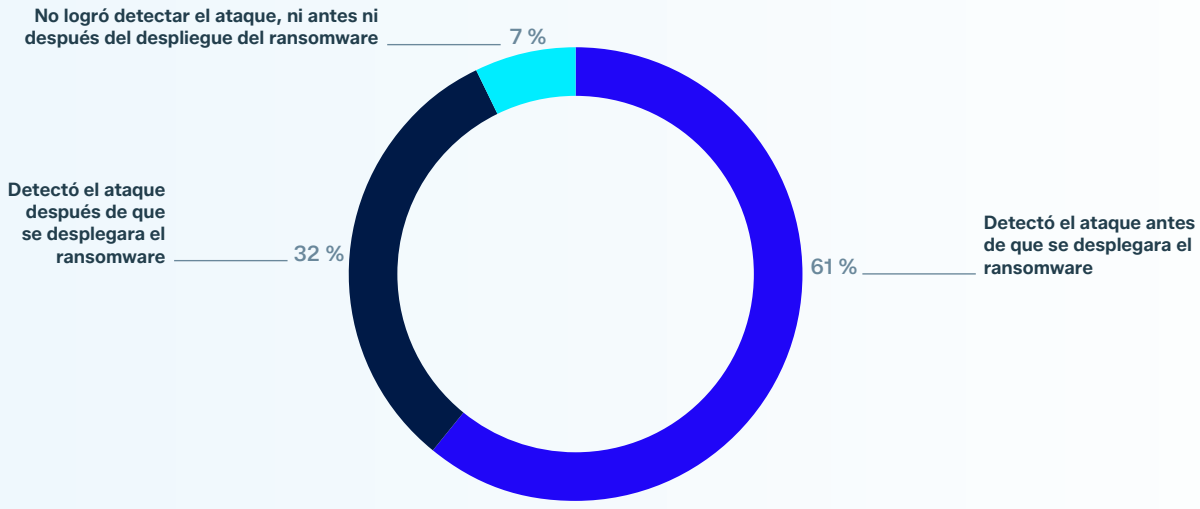
¿Por qué cree que su organización sufrió un ataque de ransomware? No teníamos suficientes expertos en ciberseguridad que supervisaran nuestros sistemas en el momento del ataque. Números base en la tabla.

NUEVA INVESTIGACIÓN

El papel de los firewalls en la defensa contra el ransomware

El 61 % de las víctimas indicaron que el firewall detectó el ataque de ransomware antes de que se activara la carga, y el 32 % afirmaron que el firewall lo identificó después de que se desplegara el ransomware. Solo el 7 % indicaron que el firewall no identificó el ataque en absoluto.

¿Qué papel desempeñó el firewall a la hora de detectar el ataque?



¿Qué papel desempeñó el firewall a la hora de detectar el ataque? n=2158

El 7 % de las víctimas cuyo firewall no detectó el ataque sufrió los peores resultados en cuanto al cifrado: el 71 % vio cifrados sus datos, frente al 50 % de los casos en los que el firewall detectó el ataque antes del despliegue del ransomware. En los casos en los que el ransomware se detectó tras su despliegue (normalmente, casos en los que se identificaron señales cuya relación con un ataque de ransomware se determinó tras producirse el incidente), el índice de cifrado de datos fue del 65 %.

Los resultados ponen de manifiesto que los firewalls desempeñan un papel fundamental a la hora de detectar ataques de ransomware, ya que los datos de telemetría de estos dispositivos proporcionan valiosas señales tempranas de la actividad de los adversarios. Cuando se combina con la información procedente de todo el entorno de seguridad —por ejemplo, de soluciones de protección para endpoints o de seguridad del correo electrónico a través de una herramienta XDR o un servicio MDR—, la telemetría de los firewalls puede ayudar a los responsables de la seguridad a detectar y bloquear los ataques de ransomware antes del cifrado de los datos.

Impacto de la detección de ataques por parte del firewall en el índice de cifrado

	Detectó el ataque antes de que se desplegara el ransomware	Detectó el ataque después de que se desplegara el ransomware	No logró detectar el ataque, ni antes ni después del despliegue del ransomware
Los ciberdelincuentes lograron cifrar los datos	50 %	65 %	71 %
Los ciberdelincuentes no lograron cifrar los datos	50 %	35 %	29 %

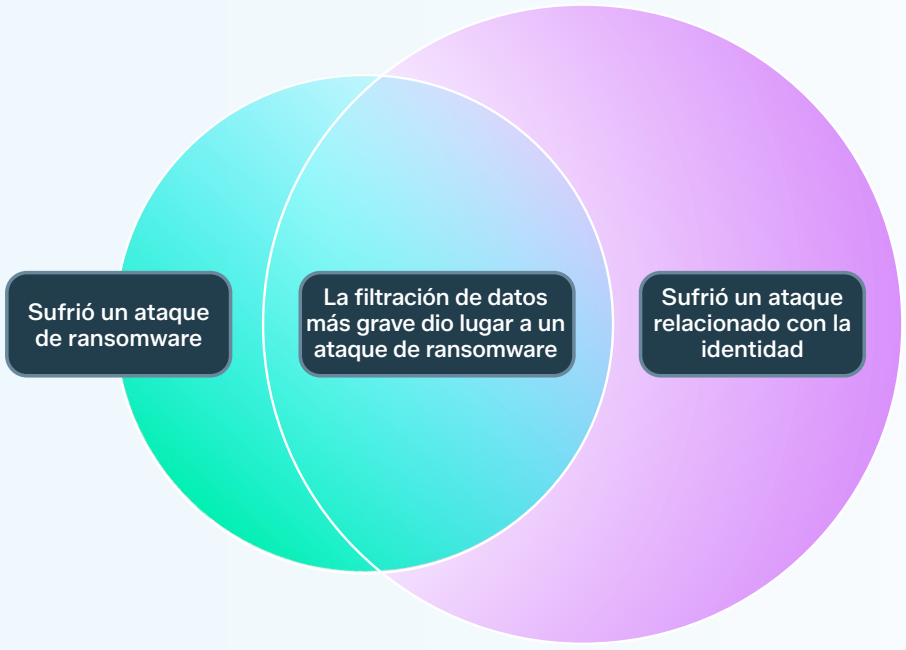
¿Qué papel desempeñó el firewall a la hora de detectar el ataque? ¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? n=2158

Los firewalls ocupan una posición muy privilegiada en la infraestructura de la organización, por lo que, en caso de que se vean vulnerados, la empresa se expone a consecuencias más graves que si se tratara de otras partes del entorno. Si los atacantes logran explotar una vulnerabilidad en el firewall, a menudo obtienen un acceso amplio a toda la empresa. La diferencia en las peticiones de rescate en estos escenarios respalda este argumento: **El 59 % de las peticiones de rescate derivadas de ataques que comenzaron con la explotación de una vulnerabilidad en el firewall ascienden a 1 millón USD o más**, frente al 48 % del total de los ataques.

NUEVA INVESTIGACIÓN

La relación entre los ataques a la identidad y el ransomware

Una de las conclusiones más llamativas de la investigación de este año es la confirmación de la relación directa entre los ataques dirigidos a la identidad y el ransomware. Entre las organizaciones que sufrieron un ataque de ransomware durante el último año, dos tercios (67 %) confirmaron que dicho incidente coincidió con su ataque más significativo a la identidad. Aunque no todos los ataques dieron lugar al cifrado de datos, esto confirma que el robo de identidad es uno de los principales mecanismos de distribución del ransomware.



Desglose de datos: en el último año, ¿se ha visto afectada su organización por el ransomware? (n=5000). ¿Ha sufrido su organización alguna filtración relacionada con la identidad en los últimos 12 meses? n=5.000. [Si ambas respuestas son afirmativas] ¿Fue este incidente de ransomware el mismo que su ataque más grave relacionado con la identidad?

Cifrado y recuperación de datos

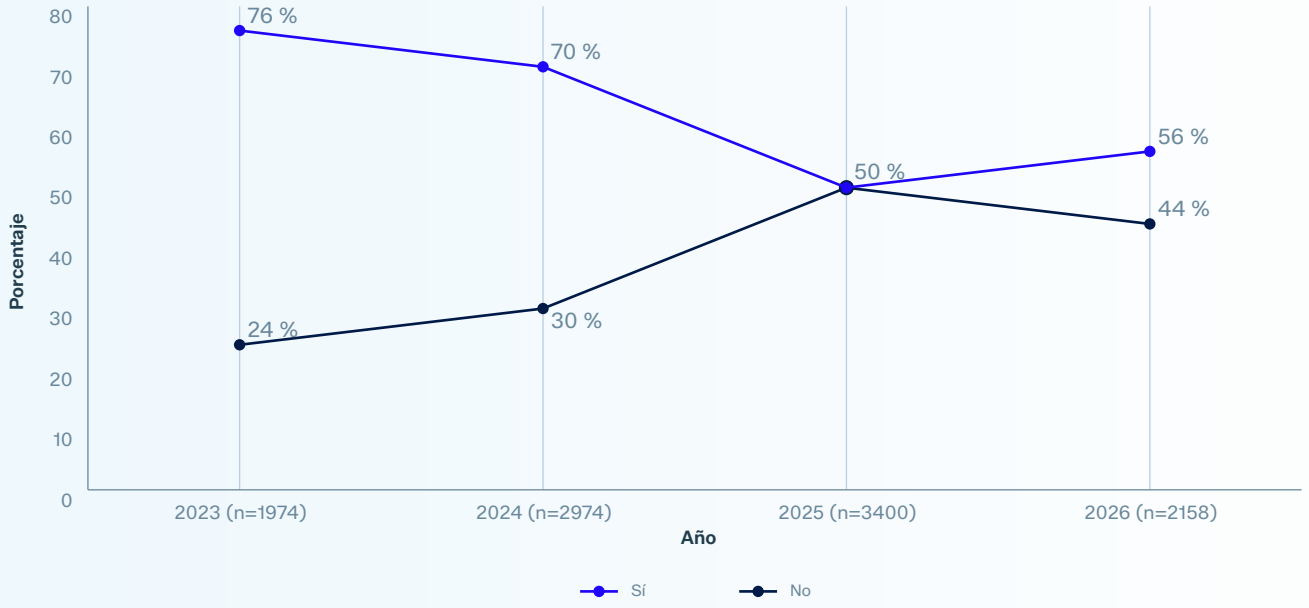
Índice de cifrado de datos

Más de la mitad de los ataques de ransomware (56 %) lograron cifrar los datos. Esto incluye un 40 % en los que solo se cifraron los datos y un 16 % en los que los datos fueron tanto cifrados como exfiltrados. El 41 % de los ataques se detuvieron antes del cifrado, mientras que el 2 % consistieron en ataques de extorsión sin cifrado.

+6 %

Aumento del índice de cifrado del ransomware con respecto al informe del año pasado.

¿Se cifraron los datos en el ataque? (Resumido: Sí/No)

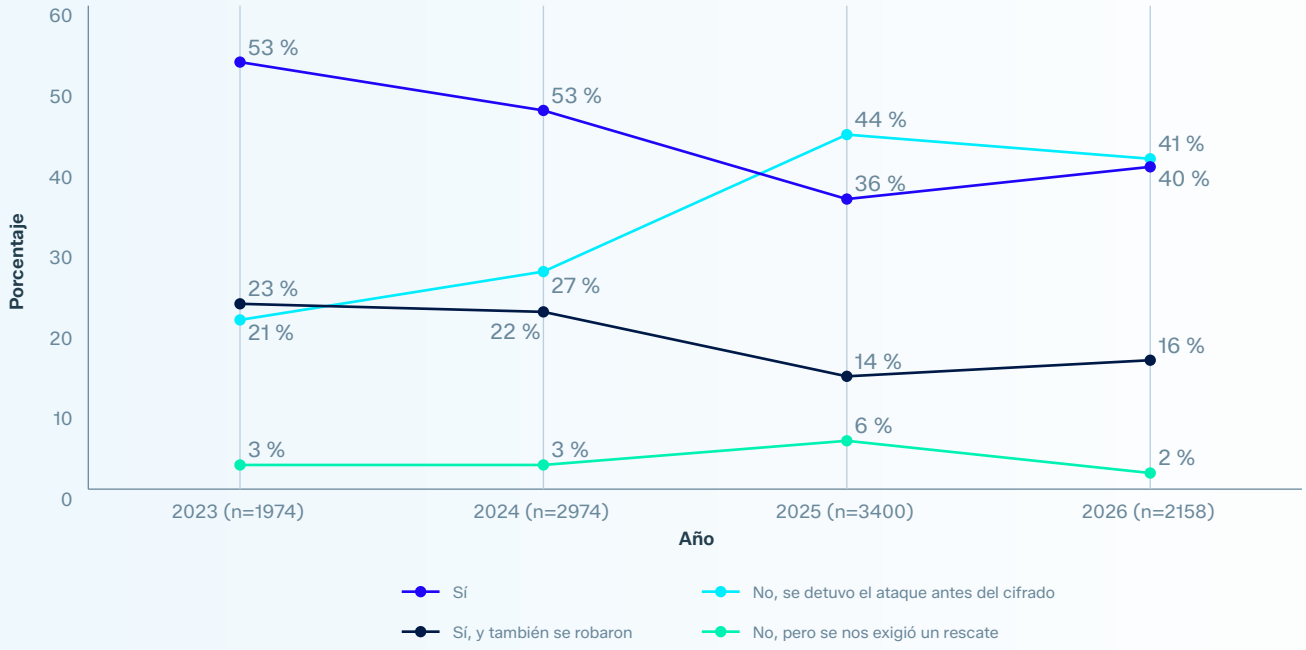


¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Respuestas resumidas: Sí / No. Números base en la tabla.

Aunque el índice de cifrado se mantiene muy por debajo del máximo del 76 % registrado en el informe de 2023, ha experimentado un ligero repunte con respecto al mínimo del 50 % registrado en el informe de 2025. Este cambio de tendencia merece atención: tras dos años de descenso en el éxito del cifrado, los atacantes parecen estar recuperando algo de terreno.

El 16 % de los ataques que combinan el cifrado y el robo de datos resulta especialmente preocupante, ya que estos ataques de doble impacto proporcionan a los atacantes múltiples puntos de presión para llevar a cabo extorsiones.

¿Se cifraron los datos en el ataque?

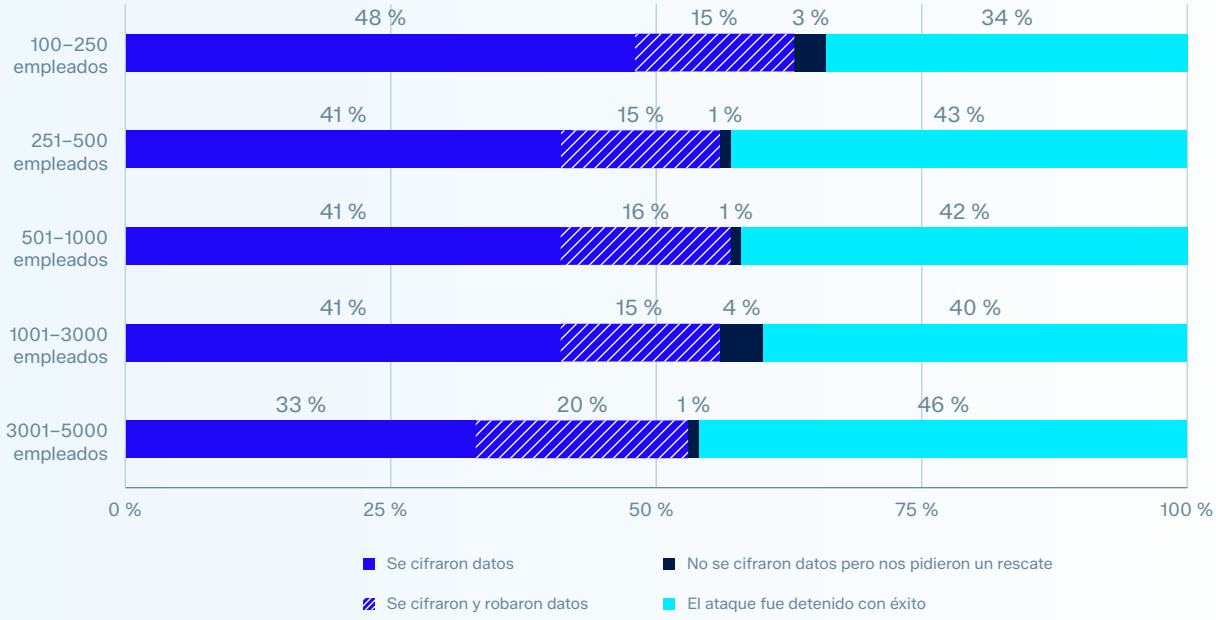


¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? (Lista completa de opciones de respuesta)
Base: organizaciones afectadas por el ransomware. Números base en la tabla.

Los resultados en materia de cifrado varía en función del tamaño de la organización: **las organizaciones más grandes encuestadas (entre 3001 y 5000 empleados) son las que tienen más probabilidades de detener los ataques antes del cifrado o la extorsión (46 %)**, frente a solo el 34 % de las más pequeñas (de 100 a 250 empleados).

Sin embargo, cuando los atacantes logran cifrar datos en las grandes organizaciones, es más probable que las víctimas sufran también un robo de datos, ya que el índice de cifrado + robo de datos alcanza el 20 % en el segmento de mayor tamaño, frente al 15 % en la mayoría de los demás. La exfiltración de datos, además del despliegue de ransomware, ofrece a los atacantes una segunda oportunidad para monetizar el ataque.

índice de cifrado de datos en los ataques de ransomware dividido por tamaño de la organización



¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? n=2158

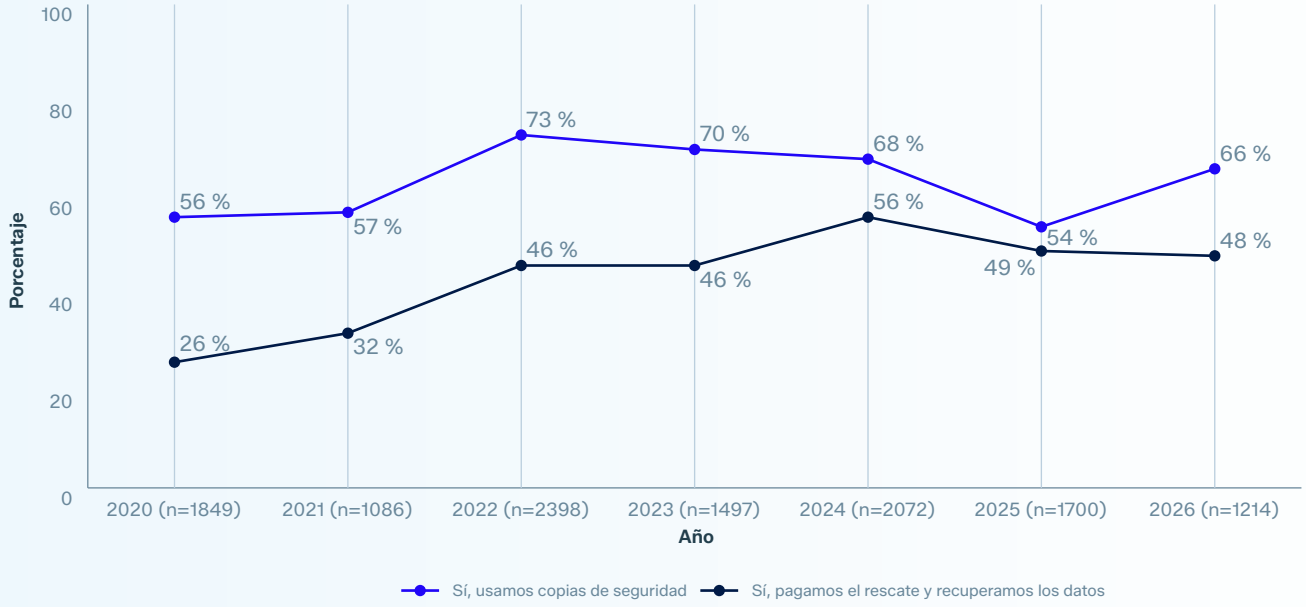
Cómo recuperaron las organizaciones los datos cifrados

La recuperación basada en copias de seguridad se disparó hasta alcanzar el 66 % de los ataques en los que se cifraron datos, frente al 54 % registrado en el informe de 2025. Este fuerte repunte sugiere que las organizaciones han renovado su inversión en infraestructura de copias de seguridad tras un descenso en su uso en 2025 y están aumentando su resiliencia frente a las demandas de rescate.

+12 %

Aumento del uso de copias de seguridad para recuperarse de ataques de ransomware entre 2025 y 2026.

Cómo recuperó su organización los datos tras los ataques de ransomware



¿Cómo recuperó su organización los datos? Base: organizaciones que sufrieron el cifrado de sus datos. Números base en la tabla. Se admiten varias respuestas, por lo que los porcentajes pueden superar el 100 %.

La proporción de organizaciones que pagaron el rescate para recuperar sus datos se redujo al 48 %, el índice más bajo de los últimos tres años. Solo el 2 % de las organizaciones indicaron que no recuperaron ningún dato, lo que pone de manifiesto que, cuando los datos están cifrados, la recuperación por cualquier medio es prácticamente generalizada.

Importe del rescate exigido e importe abonado

Peticiones de rescate

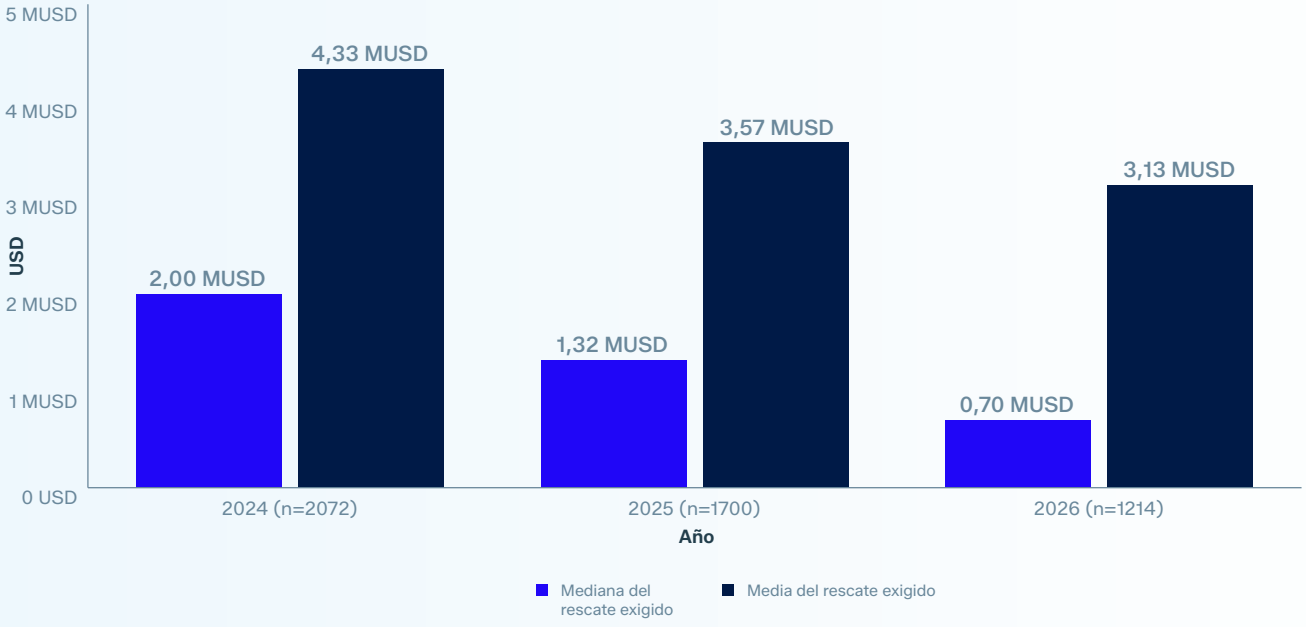
La mediana del importe de rescate exigido descendió a 698 000 USD en el informe de este año, lo que mantiene la tendencia a la baja observada desde hace varios años. Esto supone una caída del 65 % en los últimos dos años. La media de la petición de rescate también ha disminuido en este periodo, hasta situarse en 3 126 372 dólares, lo que representa una reducción del 28 % con respecto al informe de 2024.

La creciente diferencia entre la media y la mediana de los importes exigidos pone de manifiesto una distribución muy asimétrica: un pequeño número de peticiones de cuantía muy elevada inflan la media, mientras que la organización típica se enfrenta a una petición de algo menos de 700 000 USD.

698 000 USD

La mediana de las cantidades exigidas en concepto de rescate por ransomware durante el último año.

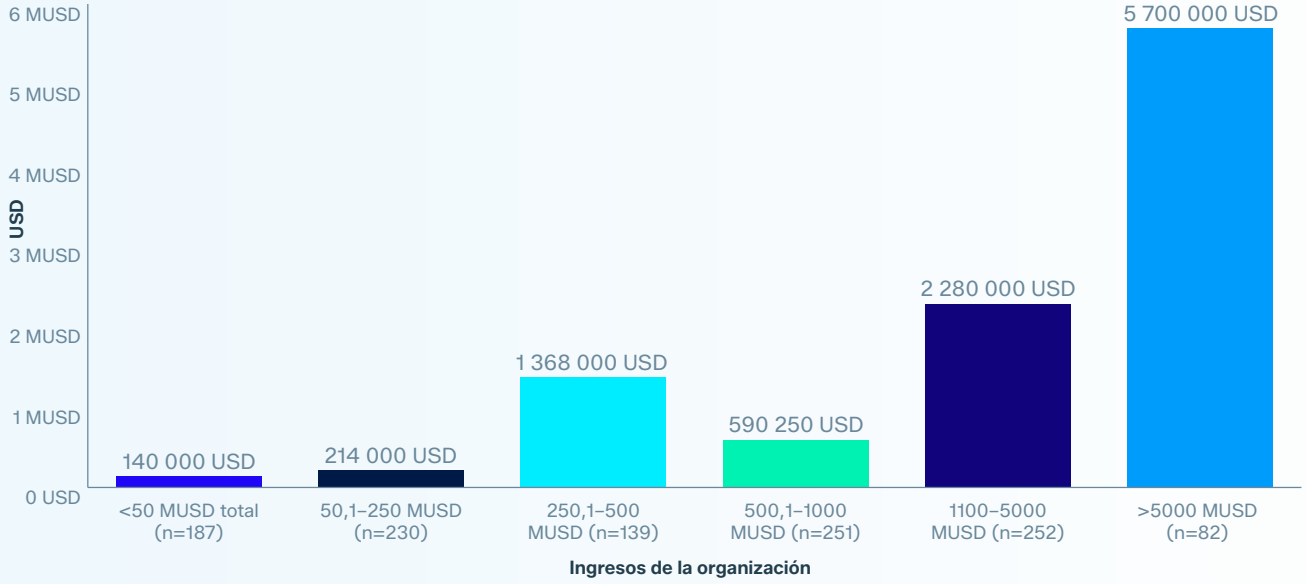
Mediana y media de las peticiones de rescate



¿A cuánto ascendía el rescate exigido por los atacantes? Base: organizaciones que sufrieron el cifrado de sus datos. Números base en la tabla. Se excluyen las peticiones atípicas de 40 millones USD o más.

Las peticiones de rescate aumentan drásticamente en proporción a los ingresos de la organización. En las organizaciones con una facturación inferior a 50 millones USD, la mediana de las cantidades exigidas en concepto de rescate fue de aproximadamente 140 000 USD. Por su parte, en las organizaciones con una facturación superior a 5000 millones USD, la mediana alcanzó los 5,7 millones USD. Este patrón apunta claramente a que los atacantes llevan a cabo una labor de reconocimiento para ajustar sus exigencias en función de la capacidad de pago que perciben.

Petición de rescate (mediana)



¿A cuánto ascendía el rescate exigido? Base: organizaciones que sufrieron el cifrado de sus datos. Números base en la tabla. Se excluyen las peticiones atípicas de 40 millones USD o más.

Importes de rescate

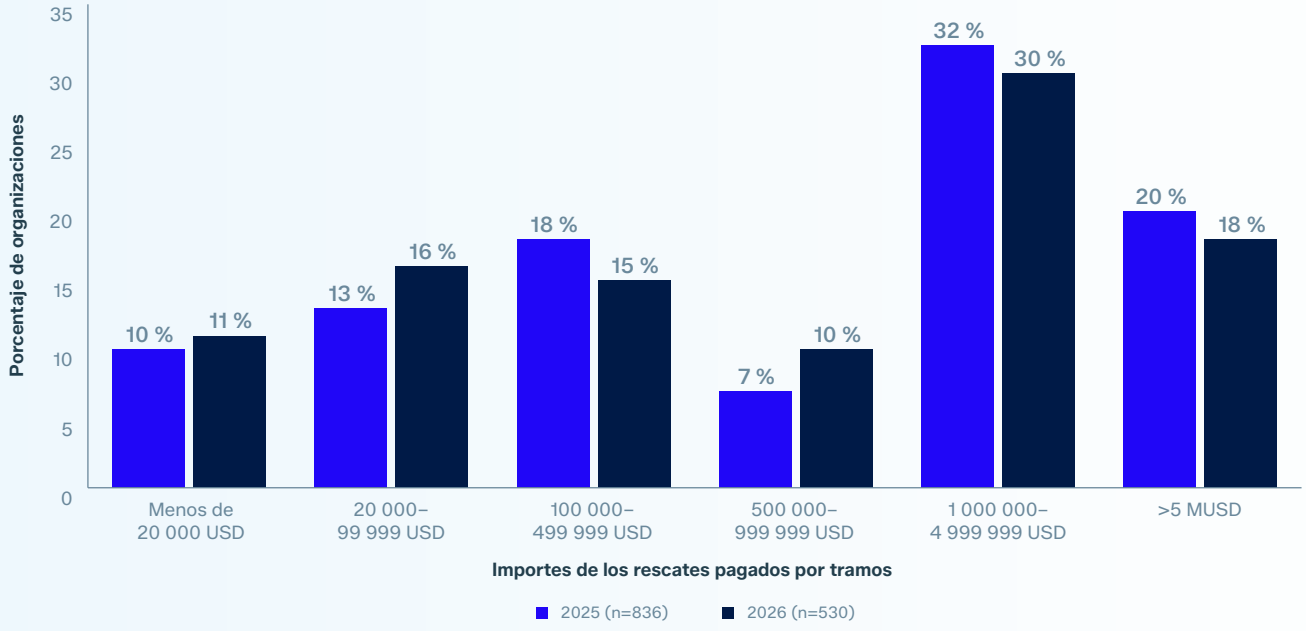
Las 530 organizaciones que pagaron el rescate nos han facilitado el importe: la mediana del importe abonado ha sido de 769 000 USD, lo que supone una caída considerable con respecto al millón USD registrado el año pasado. Poco menos de la mitad (48 %) de los pagos fueron de 1 millón USD o más, una cifra inferior al 52 % del año anterior.

El análisis de la distribución completa de los pagos revela una clara tendencia hacia la parte media del rango. Los dos tramos más elevados (entre 1 y 5 millones USD y más de 5 millones USD) registraron descensos con respecto al informe del año pasado, mientras que los tramos comprendidos entre 20 000 y 99 999 USD y entre 500 000 y 999 999 USD han aumentado cada uno, lo que sugiere que los atacantes y las víctimas se ponen cada vez más de acuerdo en pagos de cuantía baja a media.

769 000 USD

La mediana de las cantidades abonadas en concepto de rescate por ransomware durante el último año.

Importes de los rescates pagados por tramos

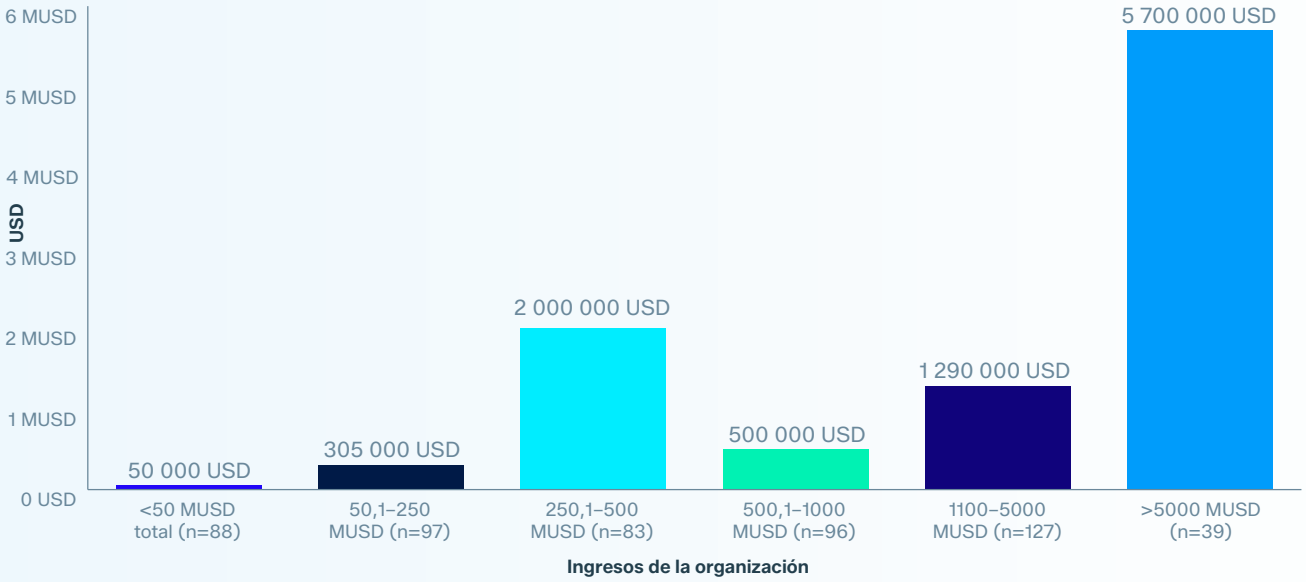


¿Cuál fue el importe del rescate que pagó su organización a los atacantes? Números base en la tabla.

Al desglosar los pagos de rescates en función de los ingresos de las organizaciones, se observó un repunte en el segmento de entre 250,1 y 500 millones USD, en el que las víctimas pagaron una mediana de 2 millones USD. Esta cifra es superior a la de cualquier otro segmento, salvo el más importante (5000 millones USD o más de ingresos anuales), y cuatro veces mayor que la de las organizaciones cuya facturación se sitúa entre 500,1 y 1000 millones USD.

Los datos relativos a los importes de los rescates exigidos muestran un alza similar en el tramo de ingresos entre los 250,1 y los 500 millones USD, con una mediana de 1,37 millones USD, frente a los 590 000 USD del tramo superior, lo que sugiere que este segmento está especialmente expuesto a los efectos del ransomware.

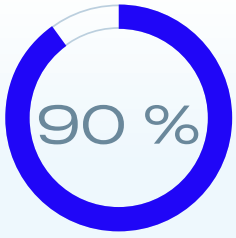
Mediana del pago de rescate



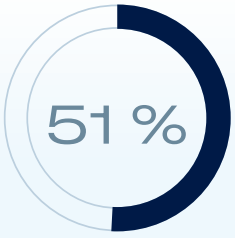
¿Cuál fue el importe del rescate que pagó su organización a los atacantes? Base: organizaciones que pagaron el rescate. Números base en la tabla.

Pagos reales frente a peticiones iniciales

507 organizaciones han revelado tanto el rescate exigido como el importe abonado finalmente, lo que pone de manifiesto la capacidad de las organizaciones para negociar con los atacantes. **La mediana del importe desembolsado se situó en el 90 % de la cifra exigida (media: 85 %)**; algo más de la mitad (51 %) pagó menos de lo exigido inicialmente, el 30 % pagó la cantidad exigida y el 18 % pagó más. Estas cifras son muy similares a las del año pasado, lo que revela que la relación entre las peticiones iniciales y los pagos reales se ha mantenido relativamente estable.

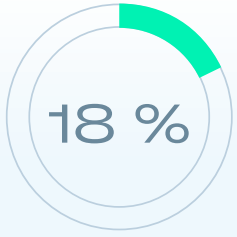


La **mediana** del importe de rescate pagado



Importes pagados **inferiores** a la petición inicial

Importes pagados que **coincidieron** con la petición inicial



Importes pagados **superiores** a la petición inicial

¿A cuánto ascendía el rescate exigido por los atacantes? ¿Cuál fue el importe del rescate que pagó su organización a los atacantes? Base: organizaciones que compartieron tanto el importe de rescate exigido como el importe desembolsado. n=507

Tal y como se ha señalado anteriormente, la mediana de las peticiones de rescate suele aumentar cuando la organización afectada tiene unos ingresos más elevados; sin embargo, los distintos tramos de ingresos presentan distintos niveles de éxito a la hora de negociar una reducción del pago final.

Las organizaciones de tamaño medio (con una facturación de entre 50 y 250 millones USD) son las que menos logran reducir el importe del rescate, ya que el 25 % de ellas paga más de lo exigido. Las empresas más grandes (con unos ingresos superiores a los 5000 millones USD) son las que consiguen negociar con mayor eficacia rescates más bajos: el 11 % paga más de lo exigido inicialmente y el 57 % paga menos, lo que supone el porcentaje más elevado de todos los grupos.

Las organizaciones que más facturan (más de 500 millones USD) logran, en mayor medida, pagar una cantidad inferior a la exigida inicialmente, lo que indica que, cuando las peticiones son más elevadas, los atacantes se muestran más dispuestos a conceder descuentos a los rescates de mayor cuantía. Las organizaciones con unos ingresos inferiores a 50 millones USD también lograron reducir, aunque de forma moderada, el importe abonado por el rescate.

Porcentaje de rescate pagado (mediana) según los ingresos de la organización

Ingresos	Proporción del rescate pagado (mediana)
<50 millones USD	95 %
50,1–250 millones USD	100 %
250,1–500 millones USD	100 %
500,1–1000 millones USD	83 %
1000-5000 millones USD	83 %
>5000 millones USD	83 %

¿A cuánto ascendía el rescate exigido por los atacantes? ¿Cuál fue el importe del rescate que pagó su organización a los atacantes?
Base: organizaciones que compartieron tanto el importe de rescate exigido como el importe desembolsado. n=507

Pagos de rescate por sector

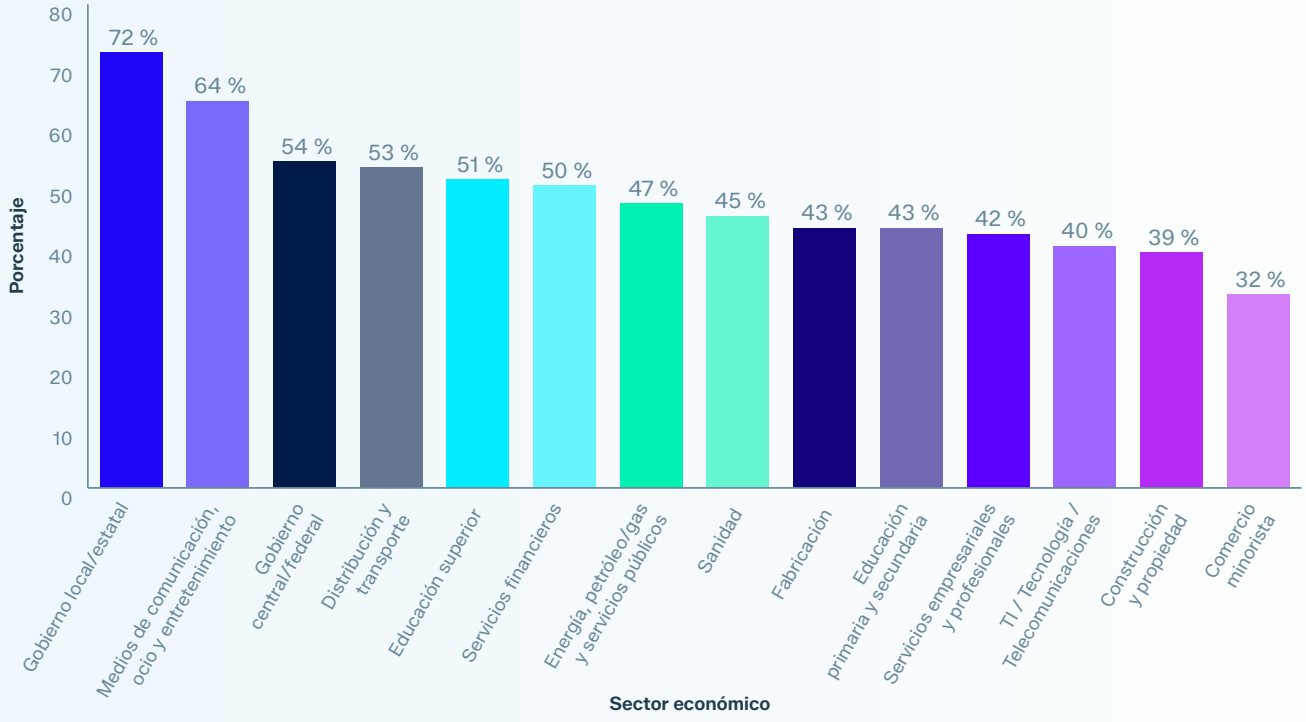
La predisposición a pagar el rescate varía según el sector. **El gobierno local/estatal (72 %) y los medios de comunicación, ocio y entretenimiento (64 %) fueron los más propensos a pagar el rescate**, con un índice más del doble que el del sector minorista (32 %).

Las organizaciones del sector público y los medios de comunicación suelen verse sometidas a una gran presión para restablecer rápidamente los servicios de atención al ciudadano o aquellos que requieren una respuesta inmediata, mientras que las empresas minoristas pueden ser más propensas a «capear el temporal».

Comercio minorista

Sector con el porcentaje más bajo de empresas que pagaron el rescate: 32 %.

Porcentaje de organizaciones que pagaron el rescate por sector



¿Cómo recuperó su organización los datos? Pagamos el rescate. Base: organizaciones que sufrieron el cifrado de sus datos. n=1214

El impacto a nivel empresarial y humano

Costes de recuperación del ransomware

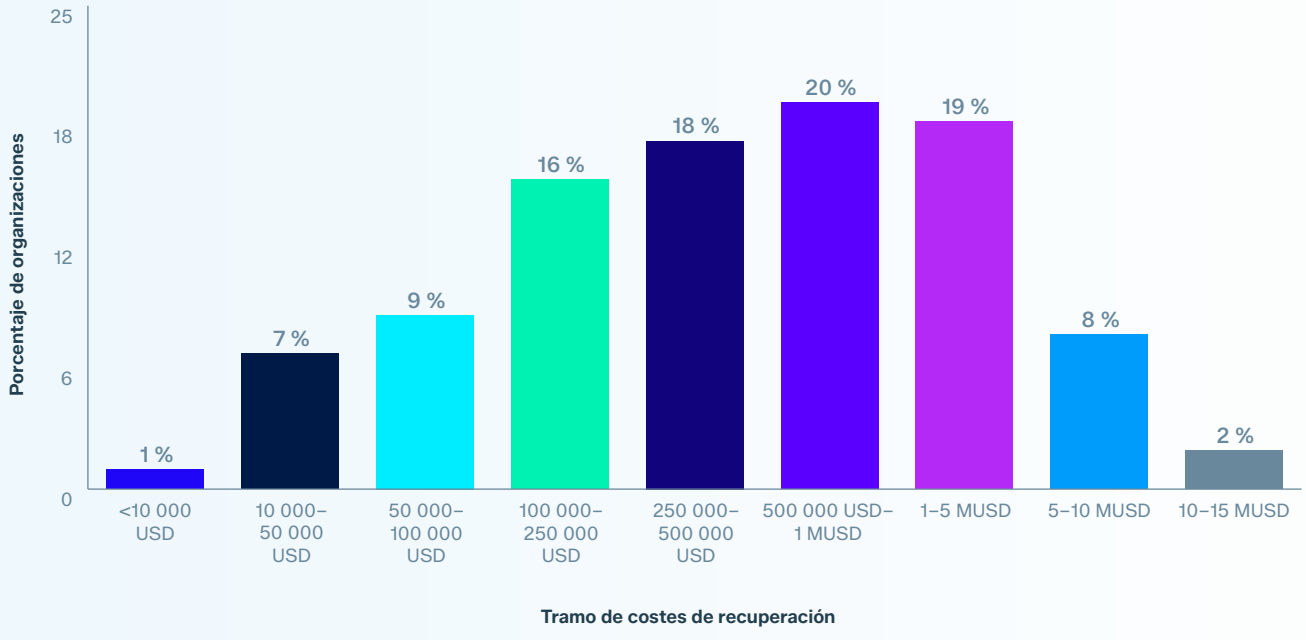
El coste medio (mediana) de recuperarse de un ataque de ransomware, sin tener en cuenta el rescate pagado, ascendió a 1 700 200 USD durante el último año. Esto supone un aumento del 11 % con respecto a la media de 1 525 716 USD del informe de 2025, aunque sigue siendo un 38 % inferior al máximo de 2 730 684 USD registrado en el informe de 2024. La mediana del coste se sitúa en 375 000 USD, sin cambios respecto al informe del año pasado.

2024	2025	2026
2,73 MUSD	1,53 MUSD	1,70 MUSD

¿Cuál fue el coste aproximado que tuvo que asumir su organización para rectificar los perjuicios del ataque de ransomware más significativo (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, etc.)? n=2158 (2026), n=3400 (2025), 2974 (2024)

Los costes de recuperación abarcan un amplio rango: el 20 % de las organizaciones incurrió en gastos de entre 500 000 y 1 millón USD, mientras que el 19 % gastó entre 1 millón y 5 millones USD.

Los costes de recuperación tras los ataques de ransomware



¿Cuál fue el coste aproximado que tuvo que asumir la organización para rectificar los perjuicios del ataque de ransomware más significativo? n=2158

Tiempo de recuperación

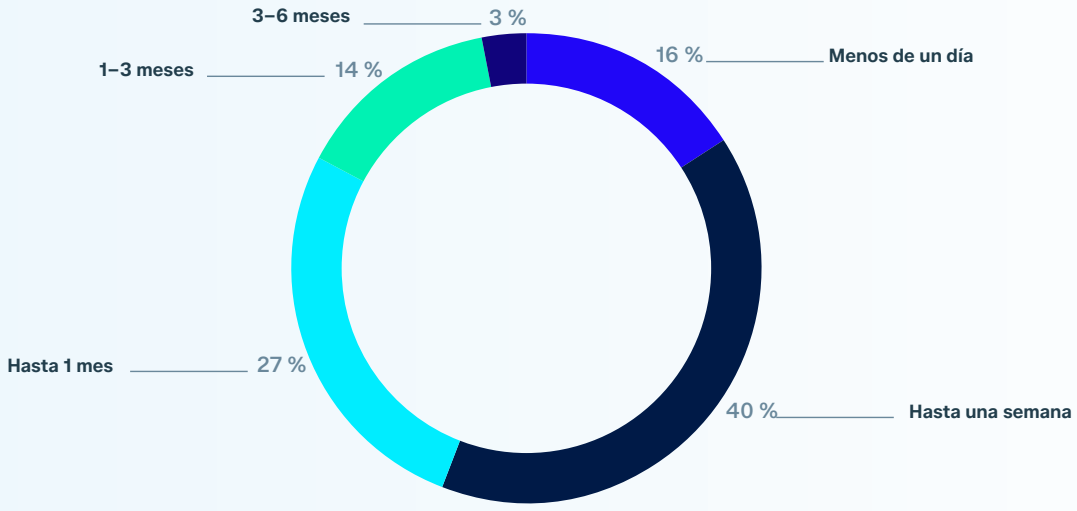
Más de la mitad de las organizaciones (55 %) se recuperaron del ransomware en el plazo de una semana (el 16 % en menos de un día) y el 83 % lo hizo en el plazo de un mes. Solo al 3 % le llevó más de tres meses.

El índice de recuperación en una semana, del 55 %, ha aumentado un 3 % con respecto al año anterior. El número medio de semanas necesarias para recuperarse se mantuvo en tres (informes de 2026 y 2025), frente a las cinco semanas que figuraban en el informe de 2024.

55 %

Porcentaje de organizaciones que se recuperaron del ataque de ransomware en el plazo de una semana.

Cuánto tiempo tardó en recuperarse



¿Cuánto tiempo tardó su organización en recuperarse totalmente del ataque de ransomware? n=2158

El impacto del ransomware a nivel humano

Prácticamente todas las organizaciones cuyos datos fueron cifrados (el 99 %) sufrieron repercusiones duraderas en sus equipos de TI y ciberseguridad. Las consecuencias más citadas fueron un aumento de la ansiedad o el estrés ante posibles ataques futuros (41 %) y una mayor presión por parte de los altos directivos (40 %). En más de una de cada cinco víctimas (el 21 %), el equipo directivo fue sustituido como consecuencia directa del ataque.

El mayor reconocimiento por parte de los altos directivos fue el único impacto que aumentó con respecto al año anterior, pasando del 31 % al 36 %. El resto de repercusiones evaluadas registraron un descenso, incluidos los cambios en las prioridades del equipo (siete puntos menos), el aumento continuo de la carga de trabajo (siete puntos menos) y la reestructuración del equipo (cinco puntos menos).

21 %

Porcentaje de equipos directivos de TI y ciberseguridad que fueron sustituidos a raíz del ataque de ransomware.

Cómo afectó el ransomware a los equipos de TI/ciberseguridad

Repercusiones	2026	Cambio con respecto a 2025
Aumento de la ansiedad o el estrés por futuros ataques	41 %	-
Aumento de la presión por parte de los cargos directivos	40 %	-
Mayor reconocimiento por parte de los cargos directivos	36 %	↑ 5 pp
Cambios en la estructura del equipo o la organización	32 %	↓ 5 pp
Cambio en las prioridades o el enfoque del equipo	32 %	↓ 6 pp
Sentimiento de culpa por no haber podido detener el ataque	31 %	↓ 3 pp
Aumento continuo de la carga de trabajo	31 %	↓ 7 pp
Bajas del personal por estrés o problemas de salud mental	29 %	↓ 2 pp
Se ha sustituido a los responsables del equipo	21 %	↓ 4 pp

¿Qué repercusiones ha tenido el ataque de ransomware en las personas de su equipo de TI/ciberseguridad? Base: Base: organizaciones que sufrieron el cifrado de sus datos. n=1214 (2026), n=1700 (2025)

El mayor reconocimiento por parte de los altos directivos puede contribuir, a su vez, a las tendencias operativas positivas observadas en otras secciones de este informe, ya que una mayor atención por parte de los directivos puede traducirse en más recursos y un mayor apoyo organizativo para los programas de ciberseguridad.

Recomendaciones

Refuerce la seguridad de la identidad como medida de defensa contra el ransomware. Dos tercios de las víctimas de ransomware confirmaron que su incidente de ransomware coincidió con su ataque más grave relacionado con la identidad, lo que pone de relieve el estrecho vínculo que existe entre la vulneración de la identidad y el ransomware. Las organizaciones deben priorizar la detección y respuesta ante amenazas relacionadas con la identidad (ITDR), aplicar la autenticación multifactor en todos los puntos de acceso y auditar periódicamente las credenciales de identidad, tanto humanas como no humanas. Tal y como mostraron los resultados de la encuesta (el 97 % de las organizaciones había habilitado la MFA de alguna forma en el momento del ataque), la MFA por sí sola no es suficiente para detener los ataques, por lo que es necesario implementarla de forma integral.

Refuerce la protección para endpoints frente a los modelos de IA de vanguardia. La IA de vanguardia está acelerando el descubrimiento de vulnerabilidades y la posibilidad de explotarlas. Es fundamental contar con defensas sólidas en los endpoints que bloqueen automáticamente los ataques basados en exploits.

Recurra a apoyo especializado o a un servicio MDR. La falta de capacidad, conocimientos y experiencia es un problema recurrente tanto para las pymes como para las grandes empresas. Hacer frente a las amenazas potenciadas por la IA supondrá una presión aún mayor en estos ámbitos, ya que los profesionales de la seguridad intentarán mantenerse al día con una tecnología de IA en rápida evolución. A menos que pueda contar con total confianza con un equipo interno de operaciones de seguridad, considere la posibilidad de colaborar con un especialista externo para cubrir esa carencia, ya sea directamente con un proveedor de MDR que ofrezca cobertura 24/7, o con un proveedor de servicios gestionados. Los proveedores capaces de resolver más incidencias íntegramente mediante la IA y la automatización también supondrán un factor multiplicador que podrá ayudarle a subsanar sus carencias en materia de conocimientos y capacidad.

Priorice la seguridad del correo electrónico. Dado que, según este informe, el phishing y los correos electrónicos maliciosos representan actualmente la mitad de las causas raíz del ransomware, las organizaciones deben implementar un filtrado avanzado del correo electrónico, aplicar los protocolos DMARC/DKIM/SPF e invertir en formación periódica sobre concienciación frente al phishing. El auge de los ataques basados en el correo electrónico sugiere que no basta con aplicar parches a las vulnerabilidades técnicas.

Invierta en infraestructura de copias de seguridad y recuperación. El año pasado, las organizaciones que contaban con sistemas de copias de seguridad sólidos recuperaron los datos cifrados a un ritmo casi sin precedentes. Las copias de seguridad deben someterse a pruebas periódicas, almacenarse fuera de línea o en formatos inmutables e integrarse en un plan de respuesta ante incidentes documentado que pueda ejecutarse en situaciones de presión.

Mantenga programas de gestión de riesgos. La reducción de 14 puntos porcentuales en el número de vulnerabilidades explotadas como causa raíz resulta alentadora, pero estos ataques siguen constituyendo un importante vector de ataque y es probable que aumenten a medida que los modelos de IA de vanguardia detecten nuevas vulnerabilidades con mayor rapidez. Las organizaciones deben mantener una cadencia rigurosa en la aplicación de parches y centrarse en medidas de mitigación, como la segmentación, Zero Trust Network Access y el despliegue de la autenticación multifactor/continua.

Reduzca la exposición a través del firewall y aproveche su telemetría para detectar los ataques de forma temprana. Asegúrese de que el firewall reciba actualizaciones rápidas (y, a ser posible, automatizadas) y minimice los servicios expuestos a Internet, como el acceso de administrador y los portales de usuario. Conecte los firewalls a soluciones XDR y MDR para que la telemetría del firewall ayude a detectar los ataques de ransomware antes de que despliegen las cargas.

Apoye a los equipos de ciberseguridad tras el incidente. El coste humano del ransomware es prácticamente universal: el 99 % de los equipos afectados ha manifestado sentir las consecuencias. Las organizaciones deben establecer protocolos claros de apoyo tras los incidentes y garantizar que la creciente concienciación por parte de la dirección se traduzca en una inversión sostenida en el personal, y no solo en tecnología.

Conclusión

El informe «El estado del ransomware 2026» revela un panorama de amenazas en plena transición.

Existen indicios claros de progreso: las peticiones de rescate y los importes abonados están disminuyendo, la recuperación a partir de copias de seguridad se ha disparado hasta alcanzar niveles casi récord, y las organizaciones son cada vez más eficaces a la hora de negociar las condiciones cuando deciden pagar. El drástico descenso de los ataques que explotan vulnerabilidades sugiere que la detección basada en IA y la inversión sostenida en la gestión de parches están dando sus frutos.

Quizá la señal más alentadora que se desprende de los datos sea el creciente reconocimiento por parte de los directivos de los equipos de ciberseguridad. Cuando los directivos prestan atención, los recursos no tardan en llegar. Las tendencias operativas positivas que se recogen en este informe, desde un mejor uso de las copias de seguridad hasta mejores resultados en las negociaciones, podrían reflejar precisamente esa dinámica.

Al mismo tiempo, los retos que aún persisten son considerables. Más de la mitad de los ataques de ransomware siguen logrando cifrar los datos, los costes de recuperación ascienden a una media de 1,7 millones USD por incidente y el desgaste humano que sufren los equipos de ciberseguridad es casi generalizado.

El hecho de que dos tercios de las víctimas de ransomware atribuyeran su incidente a una vulneración de identidad **subraya el papel fundamental que desempeña la seguridad de la identidad en la cadena de defensa contra el ransomware**. Las organizaciones que consideran la identidad como una capa de seguridad fundamental, en lugar de un aspecto secundario, están mejor preparadas para impedir que los ataques prosperen desde el principio.

Las organizaciones también deben prepararse para **el principal reto en materia de ciberseguridad de la próxima década: las amenazas aceleradas por IA**. Los datos ya dan una pista del motivo: el 62 % de las víctimas citó una laguna de seguridad, conocida o desconocida, como factor determinante en el ataque que sufrieron, y el 58 % señaló la falta de personal o de conocimientos. Ambas carencias cobran mayor relevancia a medida que la IA acelera la velocidad y la magnitud de los ataques, ya que los adversarios la utilizan para detectar puntos débiles con mayor rapidez y orquestar ataques contra múltiples puntos de control a la velocidad de las máquinas.

La tendencia que se desprende de los resultados de este año —desde los mejores resultados obtenidos cuando los firewalls detectaron los ataques de forma temprana hasta el aumento de la recuperación basada en copias de seguridad— apunta en una dirección clara: **cuando las defensas funcionan de forma conjunta, en lugar de hacerlo de forma aislada, los resultados mejoran**. Reducir la brecha frente a los ataques de la era de la IA dependerá menos de añadir más herramientas y más de conectar las que ya existen, de modo que el contexto, la detección y la respuesta puedan avanzar a la velocidad que las amenazas exigen actualmente.

Las organizaciones que obtendrán mejores resultados en los próximos años serán las que hayan logrado que los directivos presten atención a este problema y, al mismo tiempo, hayan adoptado sistemas de defensa integrados y basados en la IA, invirtiendo no solo en tecnología y procesos, sino también en las personas que se encargan de hacer frente a estas amenazas cada día.

Metodología

Esta encuesta fue realizada por Vanson Bourne por encargo de Sophos durante el primer trimestre de 2026. Se entrevistó a 2158 responsables de la toma de decisiones en materia de TI y ciberseguridad de organizaciones que habían sufrido un ataque de ransomware en los 12 meses anteriores, en 17 países: Estados Unidos, Brasil, Chile, Colombia, México, Reino Unido, Francia, Alemania, Italia, España, Suiza, Australia, India, Japón, Singapur, Sudáfrica y los Emiratos Árabes Unidos. Los encuestados procedían de organizaciones con entre 100 y 5000 empleados, repartidas por 15 sectores.

SOPHOS

Para obtener más información sobre el ransomware y cómo Sophos puede ayudarle a proteger su organización, visite nuestro sitio web.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

© Copyright 2026. Sophos Ltd. Todos los derechos reservados.
Constituida en Inglaterra y Gales N.º 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido.
Sophos es una marca registrada de Sophos Ltd. Otros productos y empresas mencionados
son marcas comerciales o registradas de sus respectivos propietarios.

2026-06-09 ES (DD)