SOPHOS

EL ESTADO DEL RANSOMWARE 2025

Resultados de una encuesta independiente realizada a 3400 responsables de TI y ciberseguridad en 17 países cuyas organizaciones se vieron afectadas por el ransomware en el último año.

Monográficos de Sophos. Junio de 2025

Introducción

Le damos la bienvenida a la sexta edición del informe anual de Sophos sobre el estado del ransomware, que pone de manifiesto la realidad de esta amenaza en 2025.

En el informe de este año se detalla cómo han evolucionado en los últimos 12 meses las experiencias de las organizaciones con el ransomware, tanto las causas como las consecuencias. También arroja luz sobre cuestiones hasta ahora poco exploradas, como los factores operativos que exponen a las organizaciones a los ataques y el impacto humano de los incidentes en el equipo de TI/ciberseguridad.

El informe, basado en las experiencias reales en la primera línea de combate de 3400 responsables de TI y ciberseguridad en 17 países cuyas organizaciones se vieron afectadas por el ransomware en el último año, ofrece datos clave sobre:

- Por qué sucumben las organizaciones al ransomware.
- Qué ocurre con los datos.
- Los rescates: peticiones e importes.
- El impacto del ransomware en el negocio.
- El impacto del ransomware a nivel humano.

Nota sobre las fechas del informe

Para que resulte más fácil comparar los datos de nuestras encuestas anuales, damos al informe el nombre del año en que se ha realizado la encuesta, en este caso, 2025. Somos conscientes de que los encuestados comparten sus experiencias del año anterior, por lo que muchos de los ataques a los que se hace referencia se produjeron en 2024.

Acerca de la encuesta

El informe se basa en los resultados de una encuesta independiente y desvinculada de cualquier proveedor sobre las experiencias de las organizaciones con el ransomware, encargada por Sophos y realizada por un especialista externo entre enero y marzo de 2025. Todos los encuestados trabajan en organizaciones con entre 100 y 5000 empleados, y se les pidió contestar según sus experiencias en los últimos 12 meses.

Los participantes procedían de 17 países y de una amplia gama de sectores, lo que garantiza que los resultados de la encuesta reflejen experiencias diversas en los sectores público y privado. El informe recoge comparaciones con los resultados de los informes anteriores, lo que nos permite realizar comparaciones interanuales. Todos los puntos de datos financieros son en dólares estadounidenses (USD).

Principales conclusiones

Por qué sucumben las organizaciones al ransomware

- Por tercer año consecutivo, las víctimas señalaron la **explotación de vulnerabilidades** como la causa raíz técnica más común de los ataques, habiéndose usado en el 32 % de los incidentes.
- Múltiples factores operativos contribuyen a que las organizaciones se vean afectadas por el ransomware, pero el más común es la **falta de conocimientos especializados**, citada por el 40,2 % de las víctimas. Le sigue muy de cerca la presencia de **lagunas de seguridad que la organización desconocía**, factor que contribuyó al 40,1 % de los ataques. En tercer lugar se sitúa la **falta de personal/capacidad**, que fue determinante en el 39,4 % de los ataques.

Qué ocurre con los datos

- El **cifrado de datos** registra el nivel más bajo de los últimos seis años: ahora, el 50 % de los ataques conllevan el cifrado de los datos, frente al 70 % de 2024.
- El 28 % de las organizaciones cuyos datos fueron cifrados también sufrieron la **exfiltración de datos**.
- El 97 % de las empresas a las que les cifraron los datos pudieron recuperarlos.
- El uso de **copias de seguridad** para restaurar los datos cifrados se sitúa en el índice más bajo de los últimos seis años: solo se utilizó en el 54 % de los incidentes.
- El 49 % de las víctimas **pagaron el rescate** para recuperar sus datos. Aunque representa un ligero descenso con respecto al 56 % del año pasado, se trata del segundo índice más alto de pago de rescates en seis años.

Los rescates: peticiones e importes

- En el último año, la mediana de **petición de rescate** se ha reducido en un tercio (34 %), situándose en 1 324 439 USD, en comparación con los 2 millones USD de 2024.
- La mediana del **importe del rescate pagado** ha caído un 50 % en el último año, pasando de 2 MUSD en 2024 a 1 MUSD en 2025. Este descenso se debe principalmente a la reducción del porcentaje de pagos de rescates de 5 MUSD o más, que ha bajado del 31 % en 2024 al 20 % en 2025.
- Al comparar las **peticiones de rescate frente a los importes desembolsados**, solo el 29 % afirmó que el pago final coincidió con la petición inicial. El 53 % pagó menos que la petición inicial, mientras que el 18 % pagó más.

El impacto del ransomware en el negocio

- Sin contar los rescates pagados, el **coste medio de recuperación** de un ataque de ransomware descendió un 44 % en el último año, pasando de 2,73 millones USD en 2024 a 1,53 millones USD.
- En cuanto al **tiempo de recuperación**, las organizaciones son cada vez más rápidas: el 53 % se recuperaron totalmente en una semana, frente al 35 % en 2024.

El impacto del ransomware a nivel humano

- Todas las organizaciones que sufrieron el cifrado de datos señalaron que el equipo de TI/ciberseguridad se vio **directamente afectado**:
  - Según el 41 % de los equipos de TI/ciberseguridad, han acusado un **aumento de la ansiedad o el estrés** ante futuros ataques.
  - Un tercio (34 %) afirmó que el equipo tenía **sentimiento de culpa** por no haber detenido el ataque a tiempo.
  - El 40 % asegura que ha **aumentado la presión** por parte de los cargos directivos, pero el 31 % afirma haber recibido un **mayor reconocimiento**.
  - El 31 % de los equipos se han visto afectados por las **bajas del personal** por problemas de estrés/salud mental relacionados con el ataque.
  - En una cuarta parte de los casos, **se sustituyó a los responsables** del equipo como consecuencia del ataque.

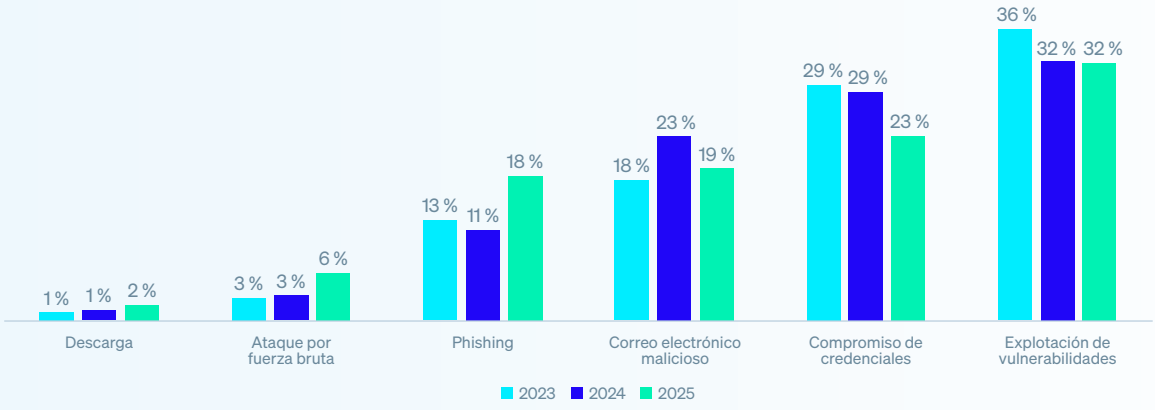
Por qué sucumben las organizaciones al ransomware

Causa raíz técnica de los ataques

Por tercer año consecutivo, las víctimas señalaron la **explotación de vulnerabilidades** como la causa raíz más común de los incidentes de ransomware: se utilizó para infiltrarse en las organizaciones en el 32 % de los ataques.

El **compromiso de credenciales** sigue siendo el segundo vector de ataque percibido más común, aunque el porcentaje de ataques que utilizaron este método descendió del 29 % en 2024 al 23 % en 2025. El correo electrónico sigue siendo uno de los principales vectores de ataque: según el 19 % de las víctimas, la causa principal fue el **correo electrónico malicioso**, y para otro 18 %, la causa fue el **phishing**, lo que supone un aumento considerable respecto al 11 % del año pasado.

Gráfico 1: causa raíz técnica de los ataques de ransomware 2023-2025

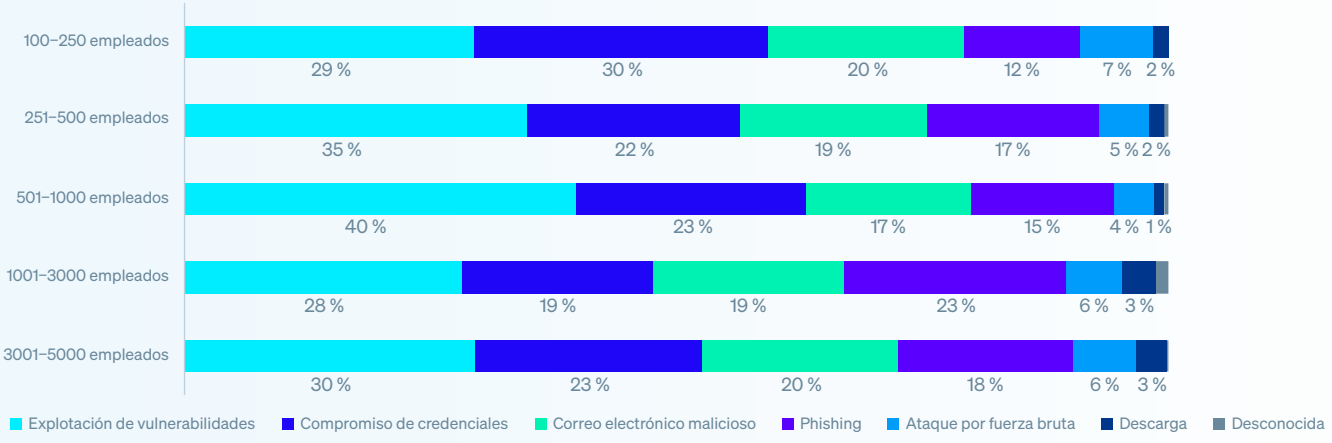


¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? - Sí. n=3400 (2025), 2974 (2024), 1974 (2023).

La investigación revela diferencias en los vectores de ataque en función del tamaño de la organización:

- El **compromiso de credenciales** fue la causa raíz más común en el segmento de 100–250 empleados, utilizado en el 30 % de los ataques.
- El 40 % de los ataques en el segmento de 501–1000 empleados fueron causados por la **explotación de una vulnerabilidad**.
- Cerca de una cuarta parte (23 %) de los ataques a organizaciones con 1001–3000 empleados comenzaron con un **correo de phishing**.

Gráfico 2: causa raíz técnica de los ataques de ransomware dividida por tamaño de la organización

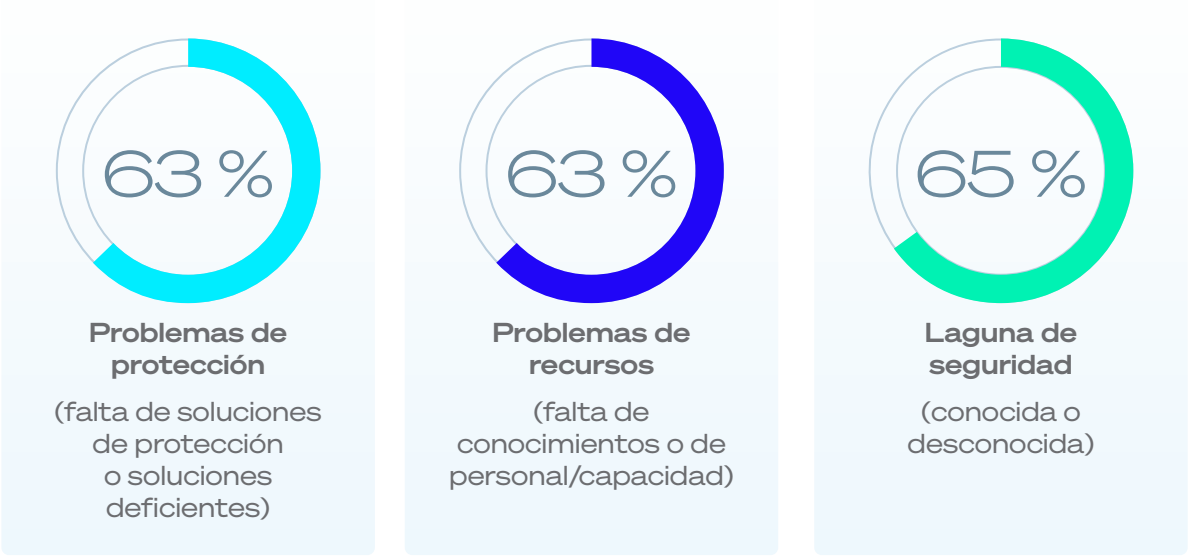


¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? - Sí. n=3400

Causa raíz operativa de los incidentes

El informe de este año explora por primera vez los factores organizativos que expusieron a las empresas a los ataques. Revela que las víctimas suelen enfrentarse a múltiples retos operativos: de media, los encuestados citaron 2,7 factores que contribuyeron a sufrir un ataque de ransomware.

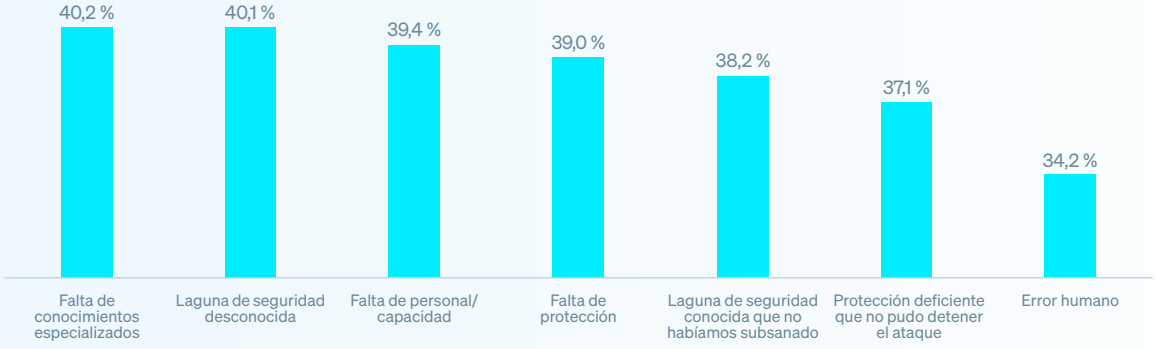
En general, no hay un único factor que destaque, ya que las causas organizativas están repartidas de forma muy equilibrada entre problemas de protección, problemas de recursos y lagunas de seguridad.



¿Por qué cree que su organización sufrió un ataque del ransomware? n=3400

La **falta de conocimientos especializados** (es decir, no tener las habilidades o los conocimientos necesarios para detectar y detener el ataque a tiempo) es la razón operativa más común, y fue nombrada por el 40,2 % de los encuestados. Le siguen muy de cerca las **lagunas de seguridad que la organización desconocía** , factor que fue crucial en el 40,1 % de los ataques. En tercer lugar se sitúa la **falta de personal/capacidad** (es decir, no disponer de un número suficiente de expertos en ciberseguridad que supervisaran sus sistemas en el momento del ataque), que fue la causante del 39,4 % de los ataques.

Gráfico 3: causa raíz operativa de los ataques de ransomware

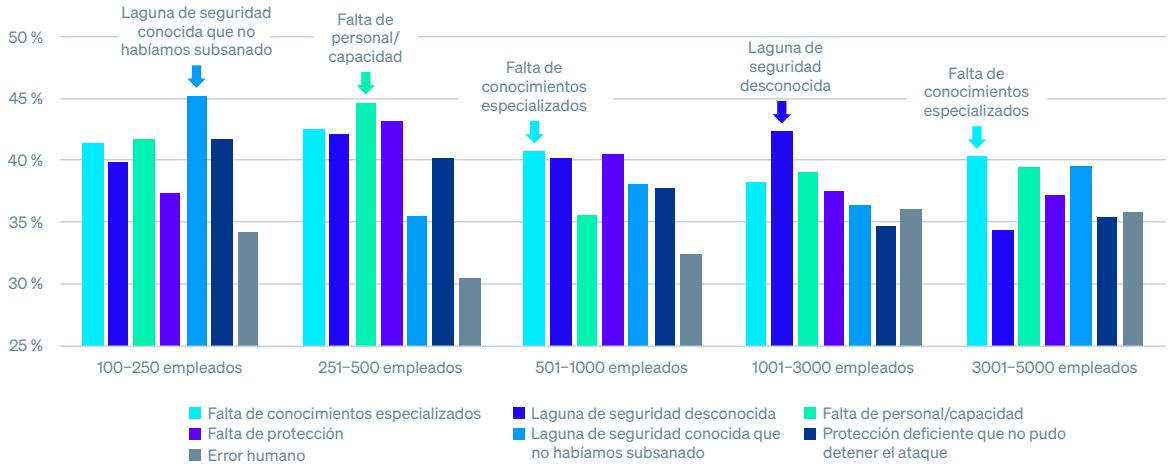


¿Por qué cree que su organización sufrió un ataque del ransomware? n=3400

Causa raíz operativa según el tamaño de la empresa

La razón operativa más común por la que las empresas se ven afectadas por un ataque de ransomware varía en función del tamaño de la organización, lo que refleja los diferentes retos a los que se enfrentan. En los cinco segmentos de tamaño de empresa utilizados en este informe, fueron cuatro los retos que más contribuyeron a sufrir un ataque, como se muestra en el siguiente gráfico.

Gráfico 4: causa raíz operativa de los ataques de ransomware dividida por tamaño de la organización



¿Por qué cree que su organización sufrió un ataque del ransomware? n=3400. Dividido por tamaño de la organización (número de empleados)

Causa raíz operativa según el sector

Del mismo modo, la causa operativa más común también varía según el sector, lo que pone de manifiesto los desafíos tan diferentes que afrontan las empresas. Cabe destacar que ningún sector señaló el error humano como la razón más común detrás del ataque.

Gráfico 5: principales causas raíz operativas de los ataques de ransomware por sector

FALTA DE **CONOCIMIENTOS ESPECIALIZADOS**	**LAGUNA DE SEGURIDAD** DESCONOCIDA	FALTA DE **PERSONAL/ CAPACIDAD**	FALTA DE **PROTECCIÓN**	**LAGUNA DE SEGURIDAD** CONOCIDA	**PROTECCIÓN** DEFICIENTE
No teníamos las habilidades o conocimientos necesarios para detectar y detener el ataque a tiempo	Teníamos un punto débil en nuestras defensas que desconocíamos	No teníamos suficientes expertos en ciberseguridad que supervisaran nuestros sistemas en el momento del ataque	No teníamos los productos y servicios de ciberseguridad necesarios	Teníamos puntos débiles en nuestras defensas que ya conocíamos pero que no habíamos solucionado	Nuestros productos y servicios de ciberseguridad no fueron capaces de detener el ataque
Energía, petróleo/gas y servicios públicos (43 %) Educación primaria y secundaria (42 %)* Fabricación y producción (42 %) Construcción y propiedad (41 %)*	Educación superior (más de 18 años) (49 %) Servicios empresariales y profesionales (46 %) Comercio minorista (46 %) Servicios financieros, incl. seguros (44 %)*	Educación primaria y secundaria (42 %)* Sanidad (42 %)	Servicios financieros, incl. seguros (44 %)* Gobierno local/estatal (40 %)	Gobierno central/ federal (45 %) TI, tecnología y telecomunicaciones (42 %) Construcción y propiedad (41 %)*	Medios de comunicación, ocio y entretenimiento (41 %) Distribución y transporte (41 %)

* indica la principal causa raíz conjunta de los ataques.

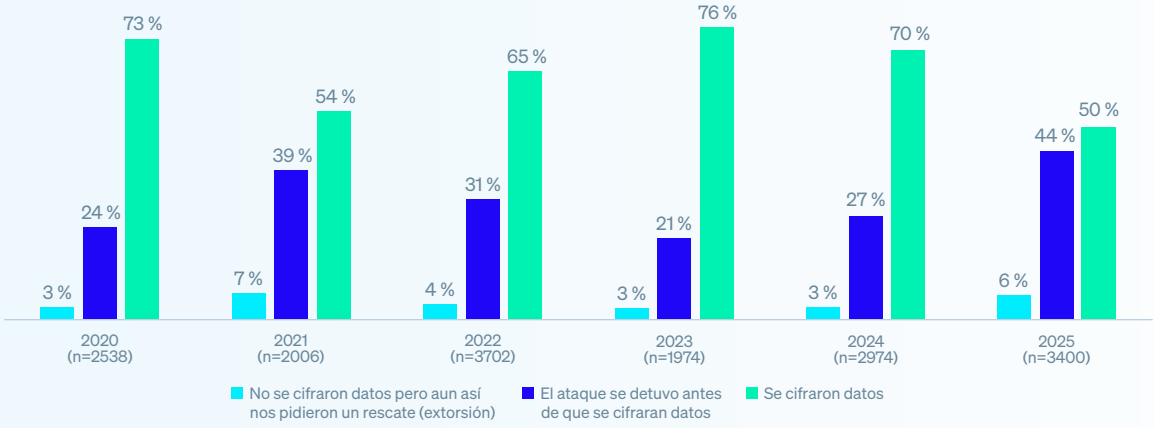
¿Por qué cree que su organización sufrió un ataque del ransomware? n=3400. Dividido por sector

Qué ocurre con los datos

Cifrado de datos

Es alentador que el cifrado de datos se sitúe en el índice más bajo registrado en los seis años que llevamos realizando este estudio: el 50 % de los ataques se saldaron con el cifrado de datos. Se ha producido un marcado descenso en el porcentaje de ataques que comportaron el cifrado de datos durante el último año, pasando del 70 % en la encuesta de 2024 al 50 % en 2025, lo que sugiere que las organizaciones están más preparadas para detener los ataques antes de que se despliegue la carga cifrada.

Gráfico 6: índice de cifrado de datos en los ataques de ransomware 2020-2025



¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Números base en la tabla.

Las organizaciones de mayor tamaño encuestadas fueron las más propensas a verse afectadas: el 65 % de los ataques a organizaciones con 3001–5000 empleados conllevaron el cifrado de datos, el índice de cifrado más alto registrado en todos los grupos por tamaño. Esto apunta a que las organizaciones grandes son menos capaces de detectar y detener el ataque antes del cifrado, y/o son menos capaces de bloquear y revertir el cifrado malicioso que las pequeñas.

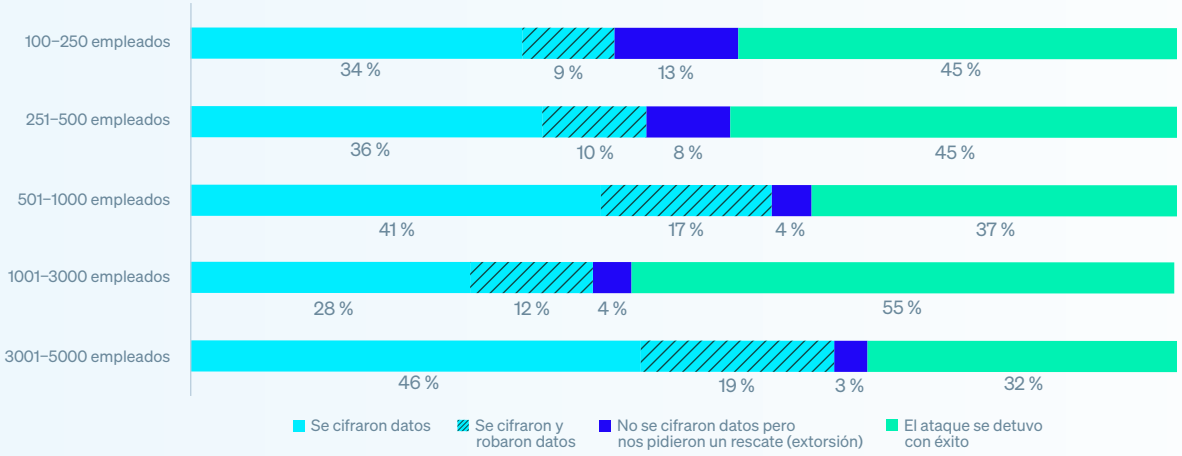
Robo de datos

Los adversarios no solo cifran los datos, sino que también los roban. El 14 % de todas las víctimas de ransomware y el 28 % de las empresas cuyos datos fueron cifrados sufrieron además el robo de datos. Si analizamos los datos en función del tamaño de la empresa, vemos que las organizaciones pequeñas tienen casi un 40 % menos de probabilidades de sufrir el robo de datos que las más grandes.

- El 22 % de las organizaciones de 100–500 empleados en que se cifraron datos también registraron el robo de datos.
- El 30 % de las organizaciones de 501–5000 empleados en que se cifraron datos también registraron el robo de datos.

Si bien es posible que las organizaciones pequeñas puedan evitar mejor el robo de datos que las grandes, esta variación puede deberse a que es más probable que los atacantes intenten exfiltrar datos de las organizaciones grandes y/o a que a las empresas pequeñas les cuesta más identificar que les han robado datos.

Gráfico 7: 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=3400

Ataques de tipo extorsión

Como se muestra en el gráfico 6, el porcentaje de organizaciones cuyos datos no se cifraron pero se les pidió un rescate de todos modos (extorsión) se duplicó en el último año: se produjo en el 6 % de los ataques en 2025, frente a solo el 3 % en 2024. En comparación con las organizaciones grandes, es más probable que se exija un rescate a las pequeñas sin que los datos se hayan cifrado (un ataque de tipo extorsión):

- El 13 % de las víctimas con 100–250 empleados sufrieron un ataque de tipo extorsión.
- El 3 % de las víctimas con 3001–5000 empleados sufrieron un ataque de tipo extorsión.

En general, las organizaciones con 1001–3000 empleados son las que mejor pueden prevenir con éxito las consecuencias de un ataque de ransomware, es decir, impedir que se cifren los datos, evitar la exfiltración de datos y evitar ser objeto de extorsión. Es posible que estas organizaciones se encuentren en un punto ideal donde son lo bastante grandes como para disponer de un mayor nivel de herramientas y conocimientos de ciberseguridad, pero no están sujetas a los mismos niveles de complejidad organizativa que las empresas más grandes.

Recuperación de los datos cifrados

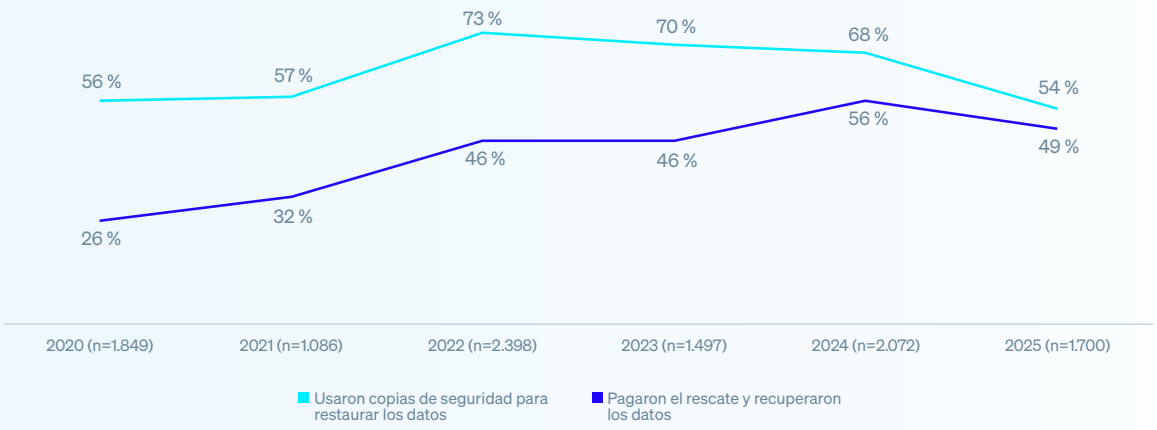
El 97 % de las organizaciones a las que les cifraron los datos pudieron recuperarlos.

Poco más de la mitad (54 %) recuperó sus datos mediante copias de seguridad, lo que supone el tercer año consecutivo en que desciende esta cifra. En general, la recuperación de datos mediante copias de seguridad se sitúa en su índice más bajo de los últimos seis años.

Algo menos de la mitad (49 %) pagó el rescate y recuperó sus datos. Aunque esto representa un pequeño descenso con respecto al 56 % del año pasado, sigue siendo el segundo índice más alto de pago de rescates de los últimos seis años.

El 29 % de las empresas cuyos datos fueron cifrados afirmaron haber utilizado "otros medios" para restaurarlos. Aquí probablemente se incluyen las que usaron claves de descifrado que ya se habían hecho públicas.

Gráfico 8: recuperación de datos mediante copias de seguridad e importes de rescate 2020-2025



¿Recuperó su organización los datos? Sí, pagamos el rescate y recuperamos los datos; Sí, usamos copias de seguridad para restaurar los datos.
Números base en la tabla

Rescates

Peticiones de rescate

En el último año, la mediana de petición de rescate ha descendido un tercio (34 %), situándose en 1 324 439 USD, frente a los 2 millones USD de 2024. Esta reducción se ha debido en gran medida al descenso de las peticiones de rescate de 5 millones USD o más, que han bajado del 30 % al 24 %. Aunque esta bajada es alentadora, es importante tener en cuenta que el 57 % de las peticiones de rescate fueron de 1 millón USD o más.

Las peticiones de rescate aumentan en función de la facturación de la organización, lo que sugiere que los adversarios "ponen precio" a sus peticiones de rescate según la capacidad de pago percibida de su víctima:

- 109 670 USD: Mediana de petición de rescate para organizaciones con ingresos anuales de 10–50 millones USD.
- 5 500 000 USD: Mediana de petición de rescate para organizaciones con ingresos anuales superiores a 5000 millones USD.

Gráfico 9: peticiones de rescate divididas por ingresos anuales de la empresa

¿A cuánto ascendía el rescate exigido por los atacantes? Números base en la tabla.

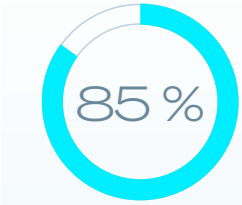
Importes de rescate

La mediana del importe del rescate pagado ha caído un 50 % en el último año, pasando de 2 MUSD en 2024 a 1 MUSD en 2025. Como ocurre con las peticiones de rescate, este descenso se debe principalmente a la reducción del porcentaje de importes desembolsados de 5 MUSD o más, que ha bajado del 31 % en 2024 al 20 % en 2025.

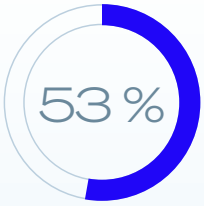
Aunque las peticiones y los importes de rescate han disminuido en el último año, es alentador que los últimos hayan registrado el mayor descenso. Dicho esto, un millón USD sigue siendo una suma muy importante, que tiene grandes consecuencias para la mayoría de las organizaciones.

Comparativa entre los importes desembolsados y la petición inicial

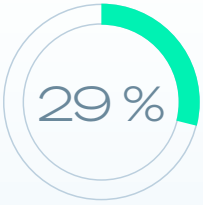
826 organizaciones que pagaron el rescate compartieron tanto la petición inicial como la cantidad pagada realmente, lo que puso de manifiesto que pagaron, de media, el 85 % de la petición de rescate inicial. En general, el 53 % pagó menos de lo que se pedía inicialmente, el 18 % pagó más y el 29 % igualó la petición inicial.



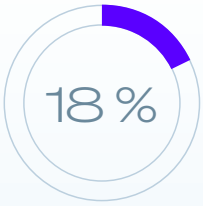
porcentaje **que se pagó** de la petición de rescate, de media



de los importes de rescate pagados fueron **inferiores** a la petición inicial



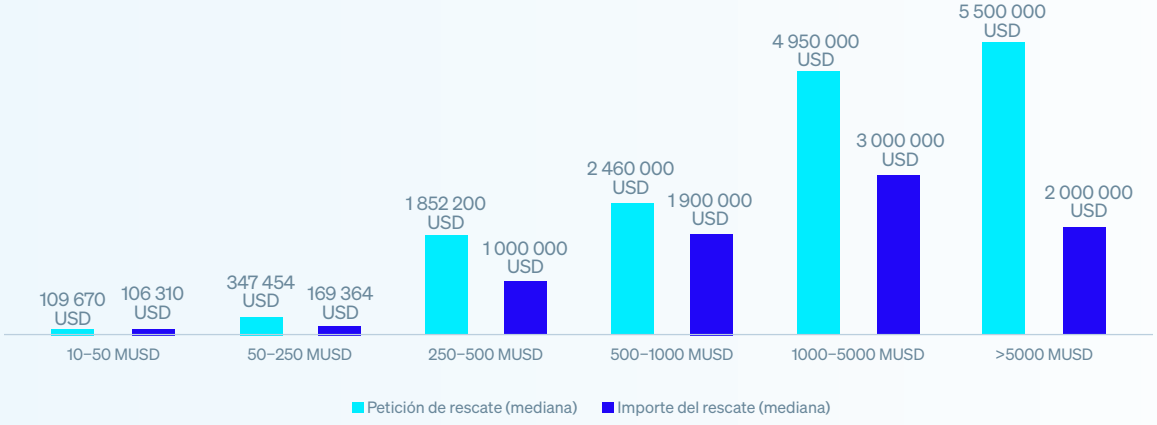
de los importes de rescate pagados **coincidieron** con la petición inicial



de los importes de rescate pagados fueron **superiores** a la petición inicial

Dividiendo los datos por ingresos anuales, vemos que todos los grupos de ingresos pagaron, de media, menos que la petición inicial. Sin embargo, las organizaciones con mayores ingresos (5000 millones USD o más) registraron el mayor descenso: el importe medio pagado (2 millones USD) representó solo el 36 % de la petición inicial (5,5 millones USD), si se excluyen los valores atípicos. Por el contrario, las organizaciones con ingresos anuales de 10–50 millones USD registraron el menor descenso: la mediana del importe pagado supuso el 97 % de la mediana de petición de rescate.

Gráfico 10: petición de rescate frente al importe pagado, dividido por ingresos anuales de la empresa



¿A cuánto ascendía el rescate exigido por los atacantes? ¿Cuál fue el importe del rescate que pagó su organización a los atacantes? (n=1.552/836)

Por qué la mayoría de los importes de rescate difieren de la cantidad exigida inicialmente

Este año, por primera vez, hemos analizado por qué algunas organizaciones pagan más de lo exigido inicialmente y otras menos, lo que nos permite arrojar luz sobre un aspecto importante a la hora de hacer frente a un ataque de ransomware.

Según revelaron 151 organizaciones que **pagaron más** que la petición inicial:

- 50 %: Los atacantes creían que podíamos permitirnos pagar más.
- 48 %: Los adversarios se dieron cuenta de que somos un objetivo valioso.
- 38 %: Los atacantes se frustraron y aumentaron el precio.
- 38 %: Nuestras copias de seguridad fallaron o no funcionaron bien.
- 32 %: No pagamos lo bastante rápido, así que subió el precio.

Por lo general, las organizaciones alegaron dos factores para justificar la decisión de pagar más, lo que revela los múltiples retos a los que se enfrentan las víctimas cuando intentan recuperar sus datos.

445 organizaciones que **pagaron menos** que la petición inicial explicaron cómo consiguieron reducir el importe del rescate:

- 47 %: Negociamos una cantidad inferior con los atacantes.
- 45 %: Los adversarios redujeron su petición inicial debido a presiones externas (por ejemplo, de los medios de comunicación o de las fuerzas de seguridad).
- 45 %: Los atacantes rebajaron su petición para animarnos a pagar.
- 43 %: Nos hicieron un descuento por pagar el rescate rápido.
- 40 %: Un tercero negoció una cantidad inferior con los atacantes.

Este grupo también señaló, de media, dos factores que explican que pagaran menos por el rescate, lo que subraya aún más la situación compleja y polifacética que viven las víctimas del ransomware.

El impacto del ransomware en el negocio

Costes de recuperación

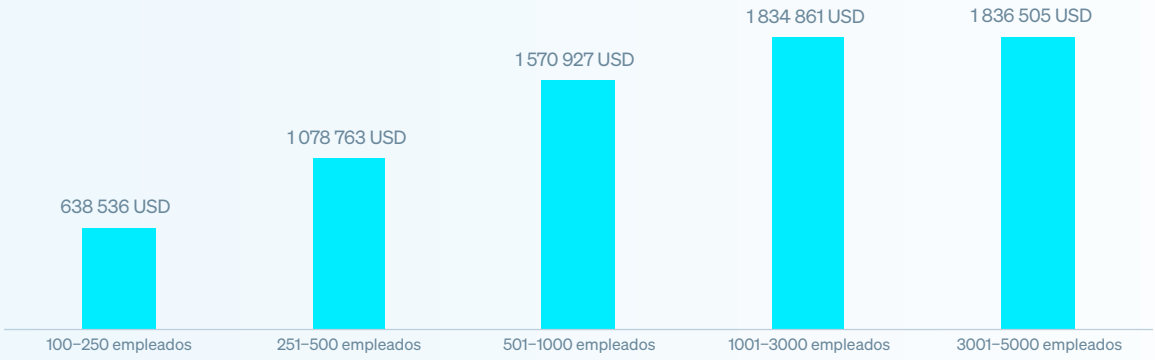
En el último año, el coste medio para recuperarse de un ataque de ransomware (sin contar el pago del rescate) descendió un 44 %, situándose en 1,53 millones USD, frente a los 2,73 millones USD de 2024. También es algo más de 300 000 USD inferior a la cifra registrada en 2023.

2023	2024	2025
1,82 MUSD	2,83 MUSD	1,53 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=3400 (2025), 2974 (2024), 1974 (2023).

Los costes de recuperación aumentan en función del tamaño de la organización hasta que se estabilizan en el caso de las organizaciones con entre 1000 y 5000 empleados. Las que tienen entre 100–250 empleados registraron un coste medio de recuperación de 638 536 USD, mientras que las que tienen entre 1000–5000 empleados incurrieron en costes de 1,83 millones USD.

Gráfico 11: coste de recuperación del ransomware dividido por tamaño de la empresa

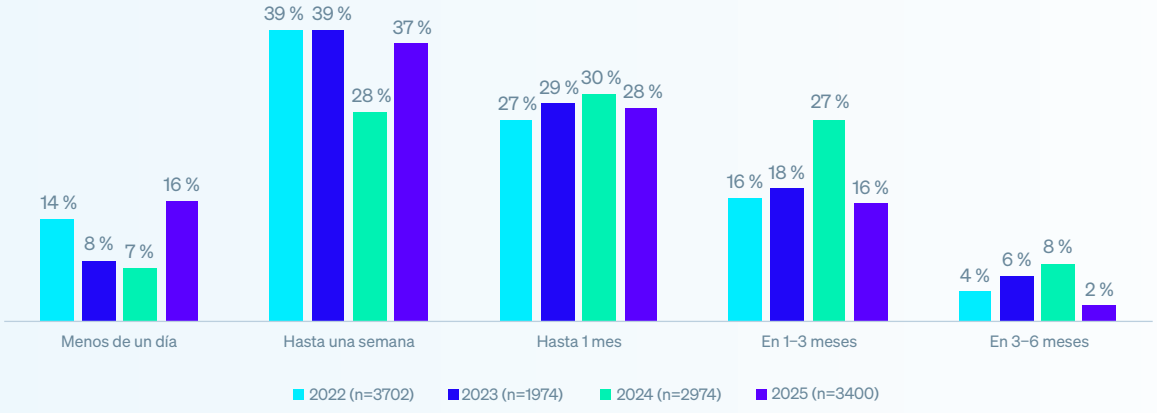


¿Cuál fue el coste aproximado que tuvo que asumir su organización para rectificar los perjuicios del ataque de ransomware más significativo (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, etc.)? n=3400

Tiempo de recuperación

Los datos revelan que las organizaciones se recuperan cada vez más rápido de los ataques: el 16 % se recuperó totalmente en un día, frente al 7 % en 2024 y el 8 % en 2023. Más de la mitad (53 %) se recuperaron en una semana, un salto significativo desde el 35 % registrado en 2024. En general, casi todas las víctimas (97 %) se habían recuperado totalmente tres meses después del ataque. Esta mejora en el tiempo de recuperación podría indicar que, durante el último año, las organizaciones han invertido en su estrategia de preparación ante ciberincidentes y en mejorar su capacidad de recuperación.

Gráfico 12: tiempo de recuperación tras ataques de ransomware 2022-2025



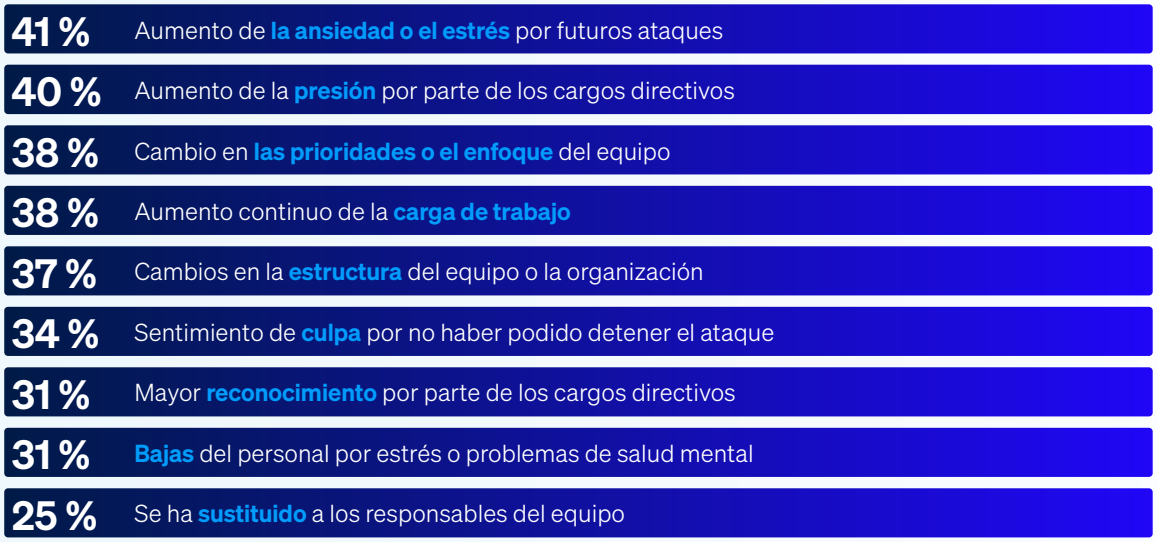
¿Cuánto tiempo tardó su organización en recuperarse totalmente del ataque de ransomware? Números base en la tabla

Como era de esperar, las organizaciones cuyos datos se habían cifrado tardaron más en recuperarse que aquellas que pudieron detener el cifrado: el 9 % de las que se habían visto afectadas por el cifrado recuperaron todos sus datos en un día, frente al 24 % de aquellas cuyos adversarios no lograron cifrar los datos.

El impacto del ransomware a nivel humano

La encuesta evidencia que sufrir el cifrado de datos en un ataque de ransomware tiene repercusiones significativas para el equipo de TI/ciberseguridad: todos los encuestados afirman que su equipo se ha visto afectado de alguna manera.

Gráfico 13: las consecuencias que tiene el cifrado de datos para los equipos de TI/ciberseguridad



¿Qué repercusiones ha tenido el ataque de ransomware en las personas de su equipo de TI/ciberseguridad, si las hay? n=1700

Recomendaciones

Aunque en el último año se han producido varios cambios en las experiencias de las organizaciones con el ransomware, sigue siendo una amenaza importante para todas ellas. A medida que los adversarios continúan redoblando y perfeccionando sus ataques, es esencial que los encargados de la seguridad y sus ciberdefensas sigan el ritmo del ransomware y otras amenazas. Las conclusiones de este informe pueden ayudarle a reforzar sus defensas, perfeccionar su respuesta a las amenazas y limitar el impacto del ransomware en su empresa y en su personal. Céntrese en estas cuatro áreas clave para adelantarse a los ataques:

- **Prevención**. La defensa más eficaz contra el ransomware es aquella en la que el ataque nunca se produce, porque los adversarios no han podido infiltrarse en su organización. Tome medidas para eliminar las causas raíz técnicas y operativas que se resaltan en este informe.
- **Protección**. Es imprescindible contar con una base sólida de seguridad. Los endpoints (incluidos los servidores) son el objetivo principal de los operadores de ransomware, así que procure que estén debidamente blindados, incluida una protección específica antiransomware para detener y revertir el cifrado malicioso.
- **Detección y respuesta**. Cuanto antes detenga un ataque, mejores serán sus resultados. Ahora, la detección y respuesta a las amenazas 24/7 es una capa esencial de defensa. Si no dispone de los recursos o las capacidades para llevarla a cabo internamente, recurra a un proveedor de detección y respuesta gestionadas (MDR) de confianza.
- **Planificación y preparación**. Contar con un plan de respuesta a incidentes que sepa bien cómo implementar mejorará en gran medida sus resultados si llega a ocurrir lo peor y sufre un ataque importante. Haga copias de seguridad de calidad y practique con regularidad la restauración de datos a partir de ellas para agilizar la recuperación en caso de sufrir un ataque.

Para descubrir cómo Sophos puede ayudarle a optimizar sus defensas contra el ransomware, hable con un asesor o visite es.sophos.com

Obtenga más información sobre el ransomware y cómo Sophos puede ayudarle a proteger su organización.

Sophos ofrece soluciones de ciberseguridad líderes en el sector a empresas de todos los tamaños, protegiéndolas en tiempo real de amenazas avanzadas como el malware, el ransomware y el phishing. Gracias a nuestras funcionalidades next-gen probadas, los datos de su organización estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

© Copyright 2025. 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 la marca registrada de Sophos Ltd. Todos los demás productos y empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.

2025-06-26 WP (DD)

SOPHOS