SOPHOS

EL ESTADO DEL RANSOMWARE EN EL SECTOR MINORISTA 2025

Resultados de una encuesta independiente realizada a 3400 responsables de TI y ciberseguridad, incluidos 361 responsables del sector minorista, en 16 países cuyas organizaciones se vieron afectadas por el ransomware en el último año.

Monográficos de Sophos. 2025 ago

Introducción

Le damos la bienvenida a la quinta edición del informe anual de Sophos sobre el estado del ransomware en el sector minorista, que pone de manifiesto la realidad de esta amenaza para las organizaciones minoristas en 2025.

En el informe de este año se desvela cómo han evolucionado en el último año las experiencias de los minoristas con el ransomware, tanto las causas como las consecuencias. También arroja nueva luz sobre cuestiones hasta ahora poco exploradas, como los factores operativos que exponen a las organizaciones minoristas a los ataques y el impacto humano de los incidentes en los equipos de TI/ciberseguridad del sector minorista.

El informe, basado en las experiencias reales en la primera línea de combate de 361 responsables de TI y ciberseguridad del sector minorista en 16 países cuyas organizaciones se vieron afectadas por el ransomware en el último año, ofrece datos clave sobre:

- Por qué sucumben las organizaciones minoristas 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 361 encuestados del sector minorista del informe se encuentran repartidos en 16 países, lo que garantiza que los resultados de la encuesta reflejan una amplia y diversa gama de experiencias. El informe recoge comparaciones con los resultados de los informes anteriores, lo que nos permite realizar una comparación interanual. 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 del sector minorista señalaron la **explotación de vulnerabilidades** como la causa raíz técnica más común de los ataques, habiéndose usado en el 30 % de los incidentes.
- Múltiples factores operativos contribuyen a que las organizaciones minoristas se vean afectadas por el ransomware, pero el más común son **lagunas de seguridad que las organizaciones desconocían**, citadas por el 46 % de las víctimas. Le siguen muy de cerca la **falta de conocimientos especializados**, factor que fue crucial en el 45 % de los ataques (la cifra más alta registrada por parte de cualquiera de los sectores analizados). En tercer lugar se sitúa la **falta de protección**, que fue determinante en el 44 % de los ataques.

Qué ocurre con los datos

- El índice de **cifrado de datos** en el sector minorista registra el nivel más bajo de los últimos cinco años: ahora, el 48 % de los ataques conllevan el cifrado de los datos, frente al máximo del 71 % alcanzado en 2023.
- El 29 % de las organizaciones minoristas cuyos datos fueron cifrados también sufrieron la **exfiltración de datos**.
- El 98 % de las organizaciones minoristas a las que les cifraron los datos pudieron recuperarlos.
- El uso de **copias de seguridad** por parte de los minoristas para restaurar los datos cifrados se sitúa en el índice más bajo de los últimos cuatro años: solo se utilizaron en el 62 % de los incidentes.
- El 58 % de las víctimas del sector minorista **pagaron el rescate** para recuperar sus datos. Aunque representa un ligero descenso con respecto al 60 % del año pasado, se trata del segundo índice más alto de pago de rescates en cinco años.

Los rescates: peticiones e importes

- En el último año, la mediana de **petición de rescate** realizada a organizaciones minoristas se ha doblado, situándose en 2 millones de USD, en comparación con la cifra de 1 millón de USD de 2024. Este importante incremento se debe principalmente al aumento del 59 % en el porcentaje de pagos de rescates por importe de 5 millones de USD o más, que ha subido del 17 % en 2024 al 27 % en 2025.
- A pesar de esto, la mediana del **rescate pagado** en el último año se ha incrementado en tan solo el 5 %, pasando de los 950 000 USD de 2024 a 1 millón de USD en 2025. Esto sugiere que, posiblemente, las organizaciones minoristas se estén resistiendo a satisfacer peticiones de rescate exageradas.
- La **proporción pagada del rescate exigido** en el sector minorista descendió hasta el 81 % en 2025 en comparación con el 85 % de 2024.
- Si se analizan detenidamente las **peticiones de rescate frente a los importes desembolsados**, solo el 29 % de los minoristas afirmó que el pago final coincidió con la petición inicial. El 59 % pagó menos que la petición inicial, mientras que el 11 % pagó más.

El impacto del ransomware en el negocio

- Para las **organizaciones minoristas, el coste medio de recuperación** de un ataque de ransomware descendió un 40 % en el último año, pasando de 2,73 millones USD en 2024 a 1,65 millones USD.
- En cuanto al **tiempo de recuperación**, las organizaciones minoristas se recuperan cada vez con mayor rapidez: el 51 % se recuperaron totalmente en una semana, frente al 46 % en 2024.

El impacto del ransomware a nivel humano

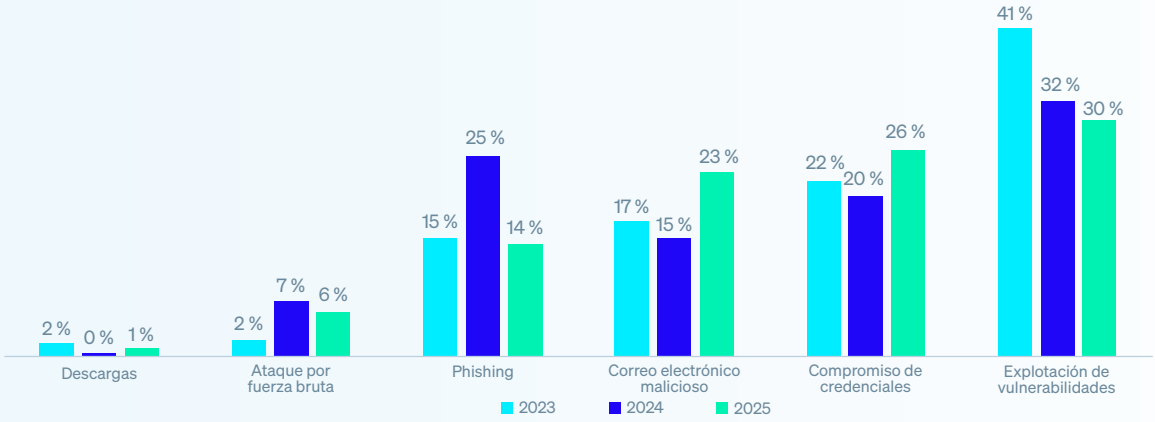
- Todas las organizaciones minoristas que sufrieron el cifrado de datos señalaron que el equipo de TI/ciberseguridad se vio **directamente afectado**:
  - Casi la mitad (47 %) de los equipos de TI/ciberseguridad del sector minorista aseguraron que ha **aumentado la presión** por parte de los cargos directivos, mientras que el 30 % afirmó haber recibido un **mayor reconocimiento**.
  - En cuanto a los impactos en los equipos de TI/ciberseguridad de los encuestados del sector minorista, el 43 % alegó tanto un aumento de la ansiedad o el estrés por futuros ataques como un **aumento continuo** de la carga de trabajo.
  - El 41 % registró cambios en la **estructura del equipo o la organización** como consecuencia del incidente.
  - El 37 % de los equipos se vio afectado por las **bajas del personal** por **problemas de estrés/salud mental** relacionados con el ataque.
  - Un tercio (34 %) afirmó que el equipo tenía **sentimiento de culpa** por no haber detenido el ataque a tiempo.
  - En una cuarta parte de los casos (26 %), **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 del sector minorista 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 30 % de los ataques. El compromiso de credenciales sigue siendo el segundo vector de ataque percibido más común, ya que el porcentaje de ataques que utilizaron este método aumentó del 20 % en 2024 hasta el 26 % en 2025. El correo electrónico sigue siendo un importante vector de ataque: según el 23 % de los minoristas, la causa principal fue el phishing (lo que supone un aumento considerable respecto al 15 % registrado en 2024), mientras que para otro 14 % la causa fue el correo electrónico malicioso.

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=359 (2025), 261 (2024), 243 (2023).

La investigación revela que a pesar de que las causas principales varían en función del sector, la explotación de vulnerabilidades es un vector importante en casi todos ellos. Excepciones importantes:

- El **phishing** fue la causa raíz más común citada tanto por instituciones de **educación primaria y secundarias** (22%) como por proveedores de **energía, petróleo/gas y servicios públicos** (29 %).
- El **compromiso de credenciales** fue el vector de ataque percibido más común por organizaciones de **gobiernos estatales y locales**, representando casi un tercio de los incidentes (32 %).

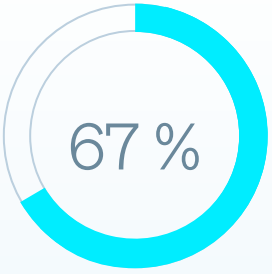
Gráfico 2: causa raíz técnica de los ataques de ransomware dividida por tamaño de la organización

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

Causa raíz organizativa de los incidentes en el sector minorista

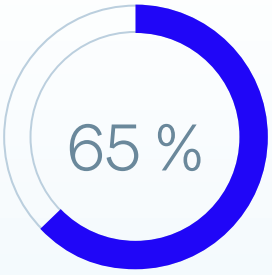
En el informe de este año se explora por primera vez los factores organizativos que expusieron a las organizaciones minoristas a los ataques. Revela que las víctimas en el sector minorista suelen enfrentarse a múltiples retos organizativos: de media, los encuestados citaron 2,9 factores que contribuyeron a sufrir un ataque de ransomware.

En general, las causas raíz organizativas están repartidas de forma muy equilibrada entre problemas de protección, problemas de recursos y lagunas de seguridad. Sin embargo, las organizaciones minoristas son un poco más propensas a citar una laguna de seguridad (conocida y desconocida) como el factor principal.



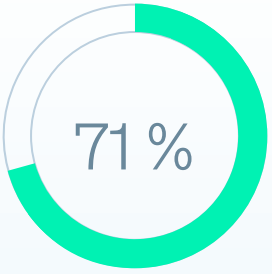
Retos de protección

Falta de protección o soluciones de protección deficientes que no pudieron detener el ataque



Problemas de recursos

La falta de experiencia humana (habilidades o capacidad) necesaria para detectar y detener el ataque a tiempo



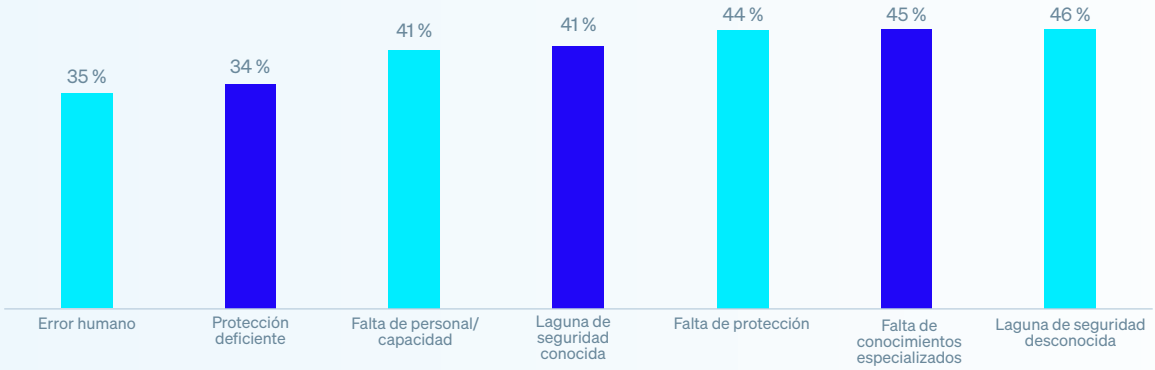
Laguna de seguridad

Tenían debilidades conocidas o desconocidas en sus defensas

¿Por qué cree que su organización sufrió un ataque del ransomware? n=361. Respuestas consolidadas.

Las **lagunas de seguridad desconocidas** (es decir, puntos débiles en las defensas que la organización desconocía) es la razón más común, y fue nombrada por el 46 % de los encuestados del sector minorista. A esta le sigue de cerca una **falta de conocimientos especializados** (es decir, carecer de las habilidades o los conocimientos necesarios para detener el ataque a tiempo), que fue determinante en el 45 % de los ataques, el índice más alto registrado por cualquier sector para esta causa raíz organizativa en concreto. En tercer lugar se encuentra la falta de protección (es decir, el hecho de no disponer de los productos y servicios de ciberseguridad necesarios), que fue la causante del 44 % de los ataques.

Gráfico 3: causa raíz operativa de los ataques de ransomware en organizaciones minoristas



¿Por qué cree que su organización sufrió un ataque del ransomware? n=361.

Causa raíz organizativa según el sector

La causa organizativa 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 de ransomware.

Gráfico 4: principales causas raíz operativas de los ataques de ransomware por sector

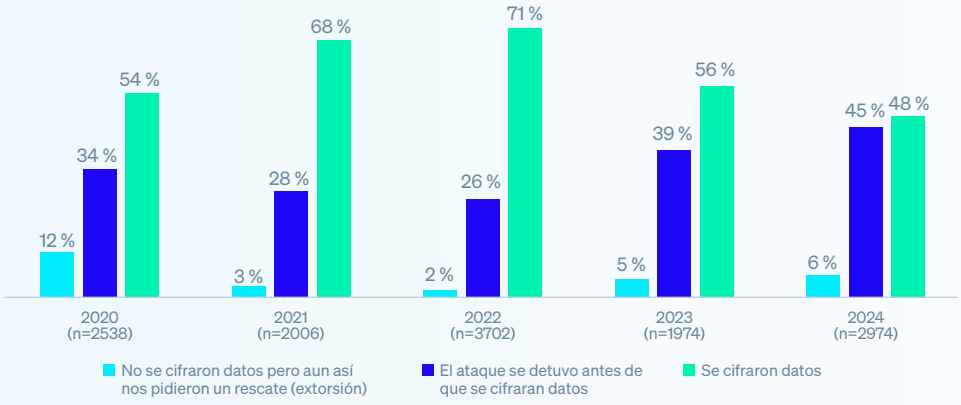
¿Por qué cree que su organización sufrió un ataque del ransomware? n=3400. Dividido por sector.

Qué ocurre con los datos

Cifrado de datos en el sector minorista

Es alentador que el cifrado de datos en las organizaciones minoristas se sitúe en el índice más bajo registrado en los cinco años que llevamos realizando este estudio, ya que algo menos de la mitad (48 %) 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 en los dos últimos años, frente al 71 % registrado en la encuesta de 2023, lo que sugiere que las organizaciones están más preparadas para detener los ataques antes de que se cifren los datos.

Gráfico 5: índice de cifrado de datos en los ataques de ransomware a organizaciones minoristas 2021 - 2025



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

Índice de cifrado de datos por sector

La organizaciones del sector de **distribución y transporte** son las que tienen más probabilidad de sufrir el cifrado de datos (64 %), lo que indica que la organizaciones de este sector están menos preparadas para detectar y detener el ataque antes del cifrado de datos y/o son menos capaces de bloquear y revertir el cifrado malicioso. En cambio, las instituciones de **educación primaria y secundaria** registraron el índice de cifrado de datos más bajo, tan solo un 29 %, lo que las sitúa muy por debajo de la media intersectorial del 50 %.

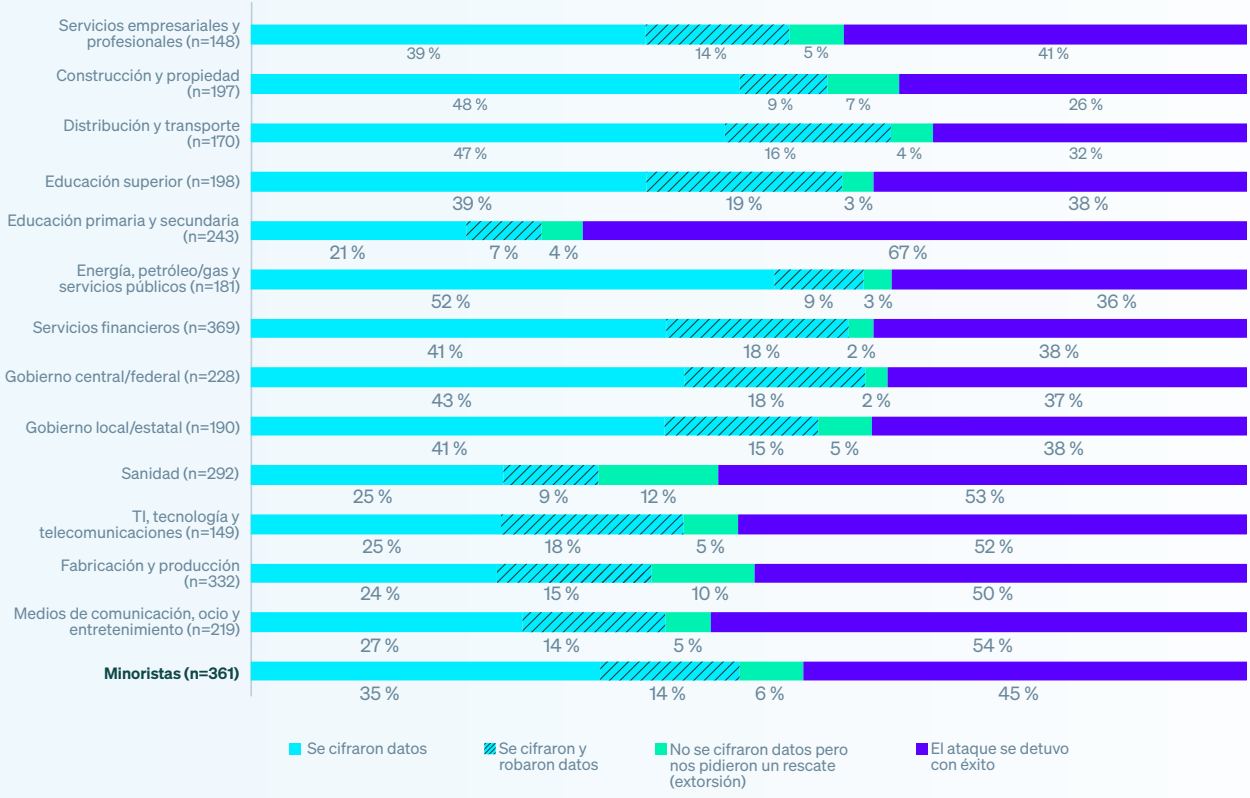
Robo de datos

Los adversarios no solo cifran los datos, sino que también los roban. En el sector minorista, el 14 % de todas las víctimas de ransomware y el 29 % de las empresas cuyos datos fueron cifrados, sufrieron además el robo de datos. Si analizamos los datos por sector vemos que:

- En el extremo superior, el 42 % de las organizaciones del sector de **TI, tecnología y telecomunicaciones** cuyos datos fueron cifrados, también sufrieron el robo de datos.
- Por el contrario, tan solo el 15 % de las organizaciones de los sectores de la construcción y propiedad, y de **energía, petróleo/gas y servicios públicos** se enfrentaron tanto al robo de datos como al cifrado.

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 6: cifrado y robo de datos por sector



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

Ataques de tipo extorsión

Como se muestra en el gráfico 5, el porcentaje de organizaciones minoristas cuyos datos no se cifraron pero se les pidió un rescate de todos modos (extorsión) se encuentra en el índice más alto en tres años: se ha triplicado pasando de tan solo un 2 % de los ataques en 2023 al 6 % en 2025.

Al analizar los datos por sector, vemos que los **proveedores de atención sanitaria** sufrieron más ataques de tipo extorsión (12 %). Esto se debe probablemente al carácter altamente sensible de los datos médicos (historiales de los pacientes, etc.). En cambio,

tanto los proveedores de **servicios financieros** como las organizaciones de **gobiernos centrales y federales** registraron la cifra más baja de estos ataques, tan solo el 2 %.

En general, las instituciones de **educación primaria y secundaria** 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.

Esto sugiere que este tipo de instituciones están demostrando ser sorprendentemente eficaces en la detección e intervención temprana, incluso cuando sus presupuestos son limitados.

Recuperación de los datos cifrados en el sector minorista

El 98 % de las organizaciones minoristas a las que les cifraron los datos pudieron recuperarlos.

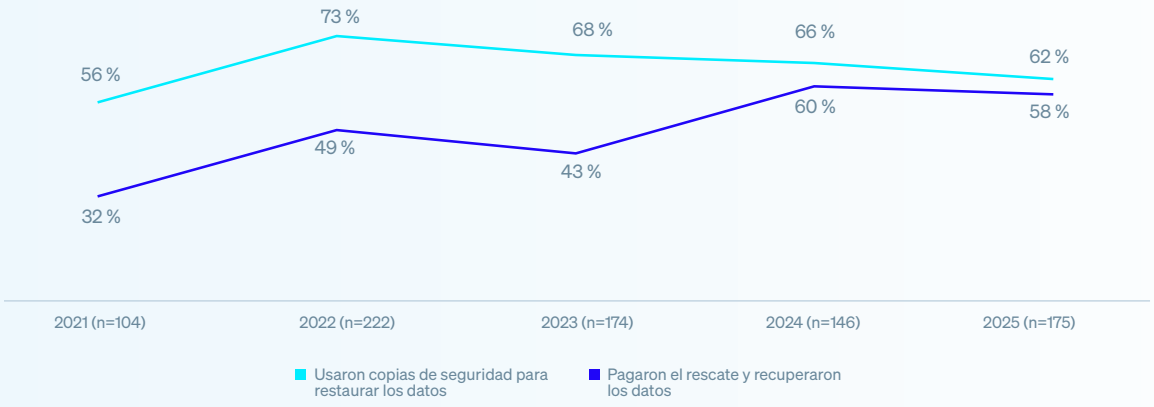
El 62 % de estas organizaciones recuperó sus datos **mediante copias de seguridad**, el índice más bajo en cuatro años, pero manteniéndose como uno de los tres sectores principales en el uso de copias de seguridad.

En este sector, el 58 % **pagó el rescate y recuperó sus datos**. Aunque esto representa un pequeño descenso con respecto al 60 % del año pasado, sigue siendo el segundo índice más alto de pago de rescates de los últimos cinco años.

La reducción de la brecha entre los minoristas que pagan el rescate para recuperar sus datos y el uso de copias de seguridad para restaurarlos, sugiere una mayor dependencia en métodos de recuperación múltiples/alternativos.

Una prueba de ello es que descubrimos que el 39 % de las organizaciones minoristas que sufrieron el cifrado de datos afirmaron que **utilizaron más de un método para restaurar sus datos**. Ningún otro sector registró un porcentaje superior.

Gráfico 7: recuperación de los datos cifrados en el sector minorista 2021 - 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 rescates en el sector minorista

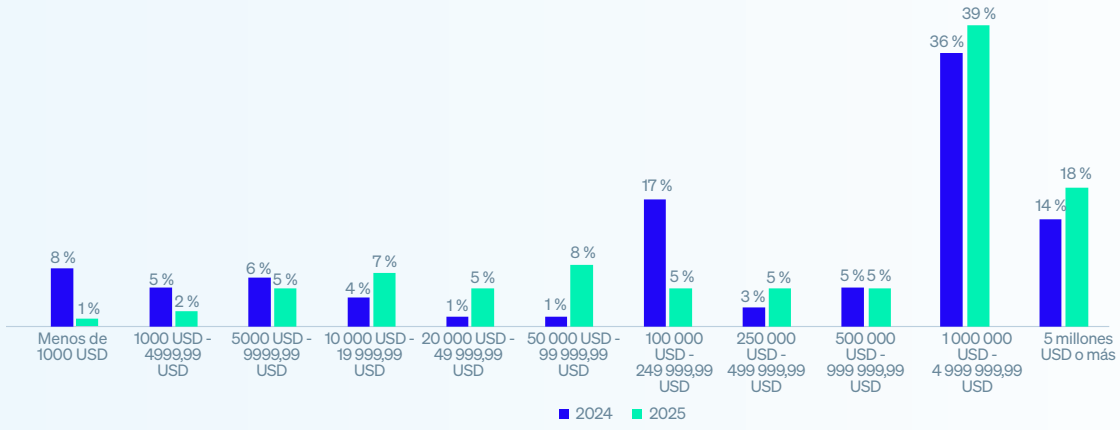
En el último año, la mediana de petición de rescate para las organizaciones minoristas se ha doblado, situándose en 2 millones USD en 2025, en comparación con 1 millón USD en 2024. En el último año, el aumento de las peticiones de rescate dirigidas a los minoristas se debe en gran medida al incremento del 59 % de las peticiones de 5 millones USD o más. Además, el 63 % de todas las peticiones de rescate realizadas a minoristas fueron superiores a 1 millón USD, un fuerte aumento en comparación al 50 % registrado en 2024.

En cambio, la media intersectorial se ha reducido en un tercio (34 %), alcanzado una cifra de 1,32 millones USD en 2025 frente a los 2 millones USD de 2024.

Importes de los rescates en el sector minorista

A pesar del fuerte aumento de las peticiones de rescate, la mediana del rescate pagado por las organizaciones minoristas se incrementó tan solo un 5 %, lo que sugiere que, posiblemente, las organizaciones minoristas se estén resistiendo a satisfacer peticiones de rescate exageradas. Sin embargo, si bien la mediana del rescate pagado se ha incrementado moderadamente, la distribución muestra una tendencia hacia pagos de rescate más altos en general, así como una clara disminución en los pagos más pequeños y un aumento en el número de organizaciones que pagan más de 1 millón USD.

Gráfico 8: importe de los rescates en el sector minorista | Distribución por bandas

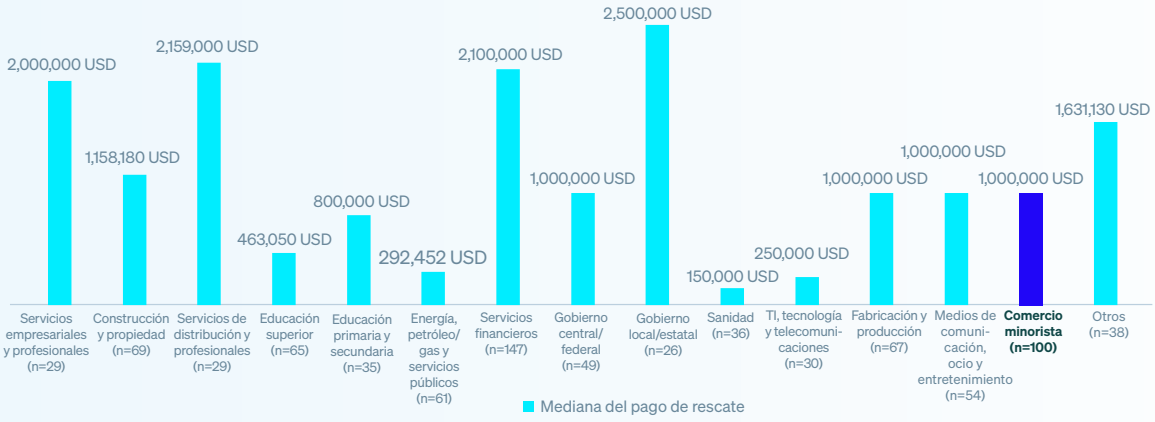


¿Cuál fue el importe de rescate que pagó su organización a los atacantes? n=100 (2025), 78 (2024)

Importes de los rescates por sector

Los importes de los rescates variaron considerablemente dependiendo del sector, siendo las organizaciones de **gobierno estatales y locales** las que pagaron el importe medio más alto a los atacantes, situándose este en 2,5 millones USD. Esto puede deberse tanto a presiones en servicios críticos, como a una ciberresiliencia limitada y a atacantes aprovechándose de la urgencia para recuperarse rápidamente. En cambio, los proveedores de **atención sanitaria** pagaron el importe más bajo, tan solo 150 000 USD.

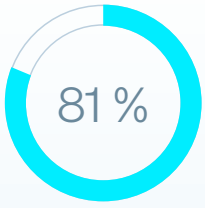
Gráfico 9: importes de los rescates por sector



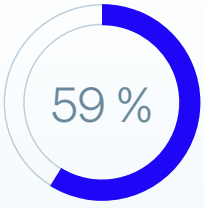
¿Cuál fue el importe del rescate que pagó su organización a los atacantes? Números base en la tabla. Nota: debido a los bajos números base en los sectores de servicios empresariales y de gobierno local/estatal, los resultados deben considerarse meramente orientativos.

Comparativa entre los importes desembolsados por los minoristas y la petición inicial

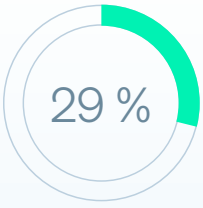
100 organizaciones minoristas que pagaron el rescate compartieron tanto la petición inicial como la cantidad pagada realmente, lo que puso de manifiesto que pagaron, de media, el 81 % de la petición de rescate inicial, un bienvenido descenso con respecto al 85 % registrado en 2024. En general, el 59% pagó menos de lo que se les solicitaba inicialmente (un porcentaje notablemente superior a la media intersectorial del 53 %), el 11% pagó más y el 29 % igualó la petición inicial.



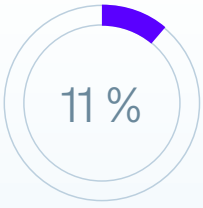
porcentaje **que se pagó** de la petición de rescate, de media



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



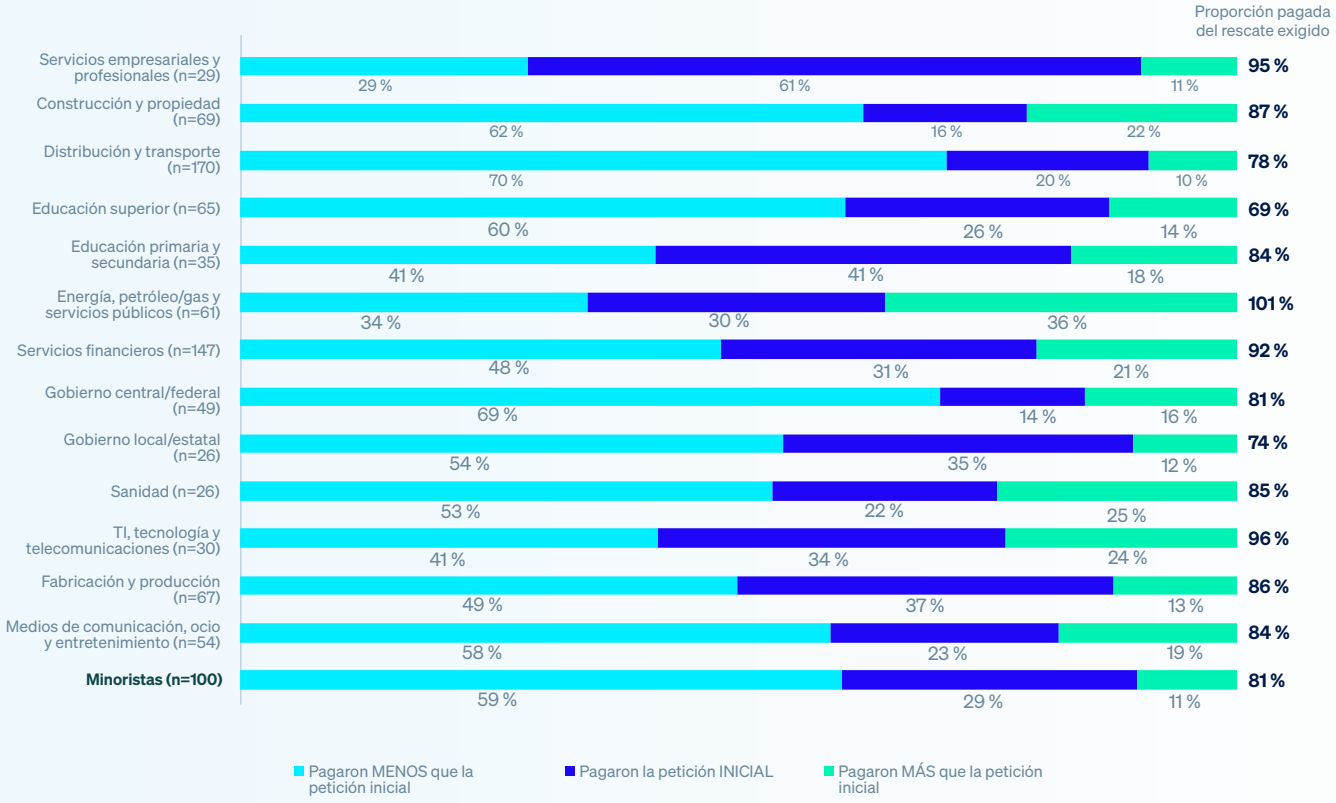
de los importes de rescate pagados **coincidieron** con la petición inicial



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

Al desglosar los datos por sector, resulta alentador ver que el resultado más común en la mayoría de los sectores es el pago de un importe inferior al originalmente solicitado. Las organizaciones del sector de **distribución y transporte** fueron con diferencia las más propensas a pagar un importe inferior a la petición original (70 %), lo que sugiere un fuerte resistencia a las peticiones de rescate. Sin embargo, los proveedores de **energía, petróleo/gas y servicios públicos** fueron los más propensos a pagar un importe superior al inicialmente solicitado (36 %), mientras que los proveedores de **servicios empresariales y profesionales** fueron más propensos a aceptar la petición de rescate inicial (61 %).

Gráfico 10: respuesta de las organización por sector



¿Cuál fue el importe del rescate que pagó su organización a los atacantes? Nota: debido a los bajos números base en los sectores de servicios empresariales y de gobierno local/estatal, los resultados deben considerarse meramente orientativos. Números base en la tabla.

Por qué la mayoría de los importes de rescate pagados por las organizaciones minoristas difieren del importe exigido inicialmente.

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

Según revelaron 11 organizaciones minoristas que **pagaron más** que la petición inicial:

- 45 %: Los atacantes se dieron cuenta de que somos un objetivo valioso.
- 45 %: Los atacantes se frustraron y aumentaron el precio.
- 45 %: Nuestras copias de seguridad fallaron o no funcionaron bien.
- 36 %: Los atacantes creían que podíamos permitirnos pagar más.
- 18 %: No pagamos lo bastante rápido, así que subió el precio.

Por lo general, las organizaciones minoristas 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.

*Importante: debido al bajo número base de organizaciones, los resultados deben considerarse meramente orientativos.

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

- 60 %: Los atacantes redujeron su petición inicial debido a presiones externas (por ejemplo, de los medios de comunicación o de las fuerzas de seguridad).
- 47 %: Los atacantes rebajaron su petición para animarnos a pagar.
- 43 %: Un tercero negoció una cantidad inferior con los atacantes.
- 42 %: Nos hicieron un descuento por pagar el rescate rápido.
- 35 %: Negociamos 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

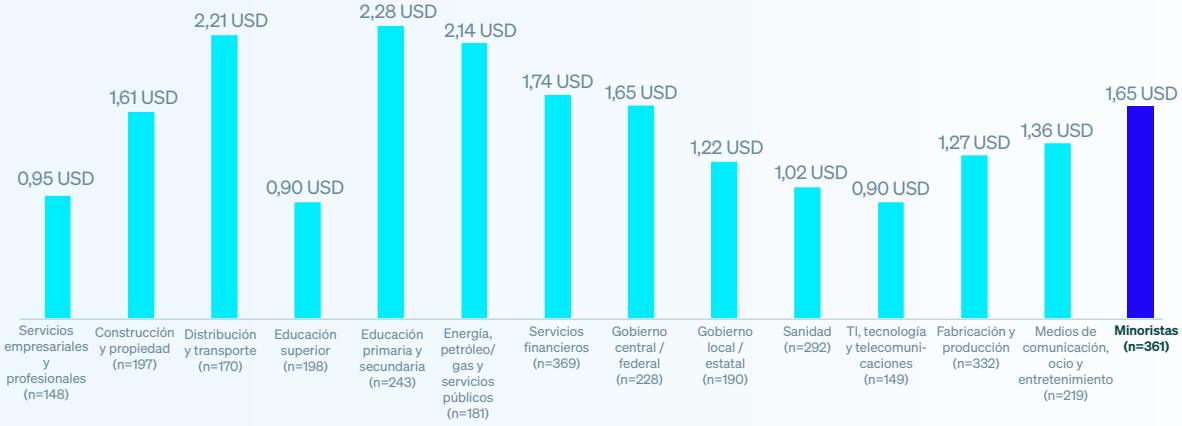
Costes de recuperación en el sector minorista

En el año pasado, el coste medio de recuperación de un ataque de ransonware para las organizaciones minoristas (sin contar el pago del rescate) ha caído hasta su punto más bajo en tres años, que fue del 40 % o 1,65 millones USD en comparación con los 2,73 millones USD de 2024. También es 200 000 USD inferior a la cifra registrada en 2023.

¿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=361 (2025), 261 (2024), 244 (2023).

Al analizar el desglose por sector, el importe de la recuperación varía notablemente. Las instituciones de **educación primaria y secundaria** registraron el coste medio más alto para rectificar incidentes, situándose en 2,28 millones USD. En cambio, tanto las instituciones de **educación superior** como las organizaciones del **sector de TI, tecnología y telecomunicaciones** registraron el coste más bajo, que se situó en 900 000 USD.

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

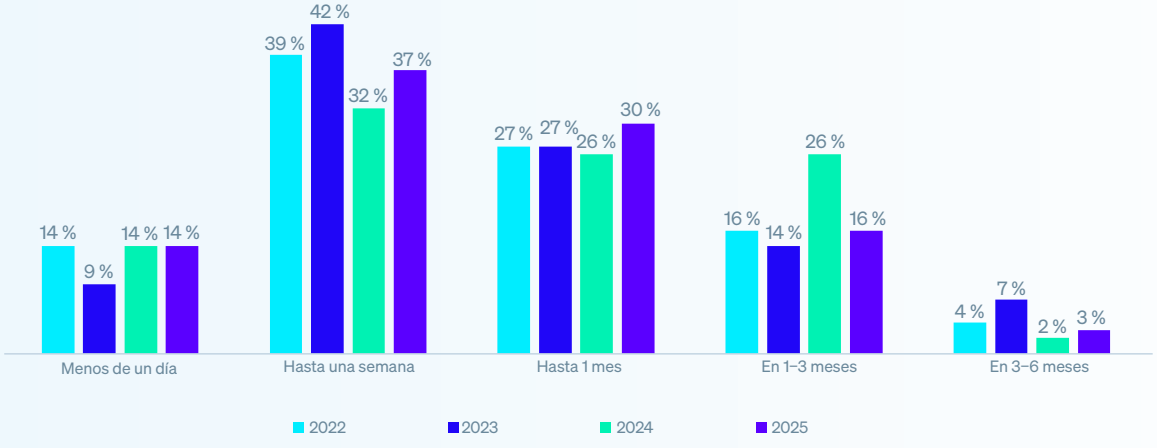


¿Cuál fue el coste aproximado que tuvo que asumir su organización para rectificar los perjuicios del ataque de ransomware más significativo (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, etc.)? Números base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

Tiempo de recuperación

Los datos ponen de manifiesto que, en 2025, las organizaciones minoristas mostraron indicios de una recuperación más rápida tras sufrir ataques de ransomware. Más de la mitad (51%) se recuperaron en menos de una semana frente al 46 % registrado en 2024. Además, la proporción de organizaciones a las que les cuesta recuperarse de uno a tres meses descendió bruscamente hasta el 16 %, frente al 26 % de 2024. En general, el 96 % de las víctimas del sector minorista se recuperaron completamente en menos de tres meses, subrayando así una creciente resiliencia y capacidades de recuperación en todo el sector.

Gráfico 12: tiempo de recuperación para las organizaciones minoristas tras ataques de ransomware 2022 - 2025



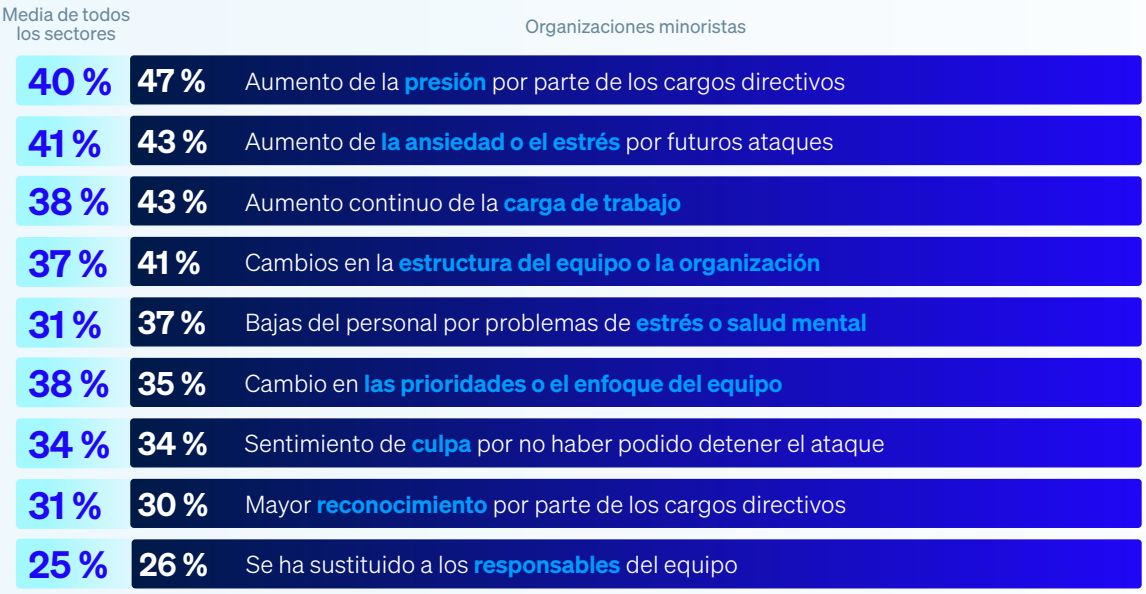
¿Cuánto tiempo tardó su organización en recuperarse totalmente del ataque de ransomware? Números base en la tabla.

Como era de esperar, las organizaciones minoristas cuyos datos se habían cifrado tardaron más en recuperarse que aquellas que pudieron detener el cifrado: el 6 % de las que se habían visto afectadas por el cifrado se recuperaron en un día, frente al 22 % 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 los equipos de Ti/ciberseguridad del sector minorista, ya que todos los encuestados afirman que sus equipos se ha visto afectados de alguna manera.

Gráfico 13: las consecuencias del 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=175

Recomendaciones

A pesar de que en el último año las organizaciones minoristas se han enfrentado de distintas maneras a un ataque de ransomware, este sigue representando una importante amenaza. 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. Adopte medidas para eliminar las causas raíz técnicas y operativas destacadas 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. Asegúrese de hacer 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.

04-08-2025 WP (MP)

SOPHOS