SOPHOS

EL ESTADO DEL RANSOMWARE EN EL SECTOR DE GRANDES EMPRESAS 2025

Resultados de una encuesta independiente realizada a 1733 responsables de TI y ciberseguridad de grandes empresas que se vieron afectadas por el ransomware en el último año.

Monográficos de Sophos. Diciembre de 2025

Introducción

Le damos la bienvenida al primer informe de Sophos sobre el estado del ransomware en las grandes empresas, que pone de manifiesto la realidad de esta amenaza para las organizaciones con más de 1000 empleados en 2025.

En el informe de este año se desvela cómo han evolucionado en el último año las experiencias de las grandes empresas con el ransomware, tanto en lo que respecta a las causas como a las consecuencias. También arroja luz sobre los factores operativos que exponen a las grandes empresas a los ataques y el impacto humano de los incidentes en los equipos de TI/ciberseguridad del sector.

El informe, basado en las experiencias reales en la primera línea de combate de 1733 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 grandes empresas al ransomware.
- Qué ocurre con los datos.
- Peticiones e importes de los rescates.
- El impacto del ransomware en el negocio.
- El impacto del ransomware a nivel humano.

Acerca de la encuesta

El informe se basa en los resultados de una encuesta independiente y desvinculada de cualquier proveedor, encargada por Sophos, sobre las experiencias de las organizaciones con el ransomware. Un especialista externo llevó a cabo la encuesta entre enero y marzo de 2025. Todos los encuestados trabajan en grandes empresas con entre 1000 y 5000 empleados, y se les pidió contestar según sus experiencias en los últimos 12 meses.

Los 1733 encuestados de grandes empresas que han participado en el informe abarcan 17 países y 14 sectores, 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 datos recogidos en los informes anteriores, lo que nos permite realizar una yuxtaposición interanual. Todos los puntos de datos financieros son en dólares estadounidenses (USD).

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 y repercusiones a los que se hace referencia se produjeron en 2024.

Principales conclusiones

Por qué sucumben las grandes empresas al ransomware

- **La explotación de vulnerabilidades** fue la causa raíz técnica más común de los ataques, utilizada en el 29 % de los incidentes. El **phishing** y la **vulneración de credenciales** le siguieron de cerca, citados en el 21 % de los incidentes.
- Son múltiples los factores operativos que contribuyen a que las grandes empresas se vean afectadas por el ransomware, pero el más común es **una laguna de seguridad desconocida**, mencionada por el 40 % de las víctimas. Le siguen muy de cerca la **falta de personal/capacidad** y la **falta de conocimientos especializados**, que fueron cruciales en el 39 % de los ataques.

Qué ocurre con los datos

- El índice de cifrado de datos en las grandes empresas registra el nivel más bajo de los últimos cinco años: **ahora, el 49 % de los ataques conllevan el cifrado de los datos**, frente al 64 % alcanzado en 2022.
- El 30 % de las grandes empresas cuyos datos fueron cifrados también sufrieron la exfiltración de datos.
- El 96 % de las grandes empresas a las que les cifraron los datos pudieron recuperarlos.
- El uso de copias de seguridad por parte de las grandes empresas para restaurar los datos cifrados se sitúa en el índice más bajo de los últimos cuatro años: solo se utilizaron en el 53 % de los incidentes.
- **El 48 % de las grandes empresas afectadas pagó el rescate** para recuperar sus datos, un porcentaje que se encuentra entre los más bajos registrados en la encuesta de este año.

Los rescates: peticiones e importes

- En el último año, la mediana de **petición de rescate** realizada a las grandes empresas se desplomó un 56 %, situándose en **1,20 millones USD** en 2025, frente a los 2,75 millones USD de 2024. La principal causa de este importante descenso es una reducción del 24 % en las peticiones de rescate de 5 millones USD o más, que pasaron del 38 % en 2024 al 29 % en 2025. No obstante, es importante señalar que las peticiones de rescate por valor de 1 a 5 millones USD aumentaron un 17 %.
- La mediana del **rescate pagado** por las grandes empresas también descendió: se situó en **1 millón USD** en 2025, frente a los 1,26 millones USD de 2024. Este descenso se debe en gran medida a la reducción del 37 % en el porcentaje de pagos de rescates por importe de 5 millones USD o más. Sin embargo, cabe destacar que se ha producido un aumento en casi todos los tramos de pagos inferiores a 5 millones USD.
- La **proporción pagada del rescate exigido** por las grandes empresas descendió del 95 % en 2024 al 86 % en 2025.
- Si se analizan detenidamente las **peticiones de rescate frente a los importes desembolsados**, casi un tercio (31 %) de las grandes empresas afirmó que el pago final coincidió con la petición inicial. El 51 % pagó menos que la petición inicial, mientras que el 18 % pagó más.

El impacto del ransomware en el negocio

- Para las **grandes empresas, el coste medio de recuperación** de un ataque de ransomware descendió un 41 % en el último año, pasando de 3,12 millones USD en 2024 a **1,84 millones USD**.
- En cuanto al **tiempo de recuperación**, este sector se recupera cada vez con mayor rapidez: en 2025, exactamente la mitad se recuperó en una semana, frente al 36 % en 2024.

El impacto del ransomware a nivel humano

Todas las grandes empresas que sufrieron el cifrado de datos señalaron que el equipo de TI/ciberseguridad se vio directamente afectado:

- El 40 % de los equipos de TI/ciberseguridad aseguró que ha **aumentado la presión** por parte de los cargos directivos, mientras que el 31 % afirmó haber recibido un **mayor reconocimiento**.
- Según el 39 % de los encuestados, se ha producido un **aumento continuo de la carga de trabajo** y **un incremento de la ansiedad o el estrés** por futuros ataques.
- Un 37 % indicó un **cambio en las prioridades o el enfoque del equipo**.
- Más de un tercio de los encuestados (35 %) señaló que las repercusiones del incidente fueron tanto un **sentimiento de culpa** por no haber podido detener el ataque, como **cambios en la estructura del equipo o la organización**.
- El 31 % de los equipos se vio afectado por las **bajas del personal** por **problemas de estrés/salud mental** relacionados con el ataque.
- En más de una cuarta parte de los casos (27 %), **se sustituyó a los responsables** del equipo como consecuencia del ataque.

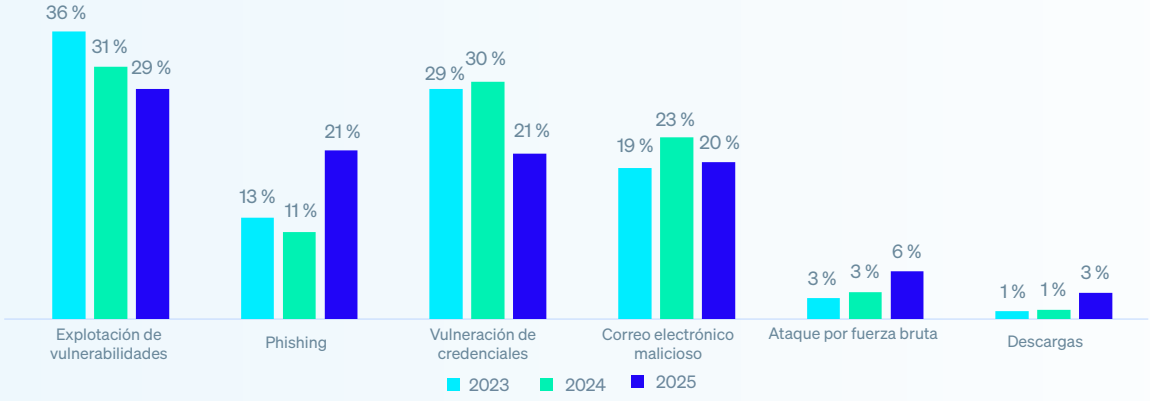
Por qué sucumben las grandes empresas al ransomware

Causa raíz técnica de los ataques en el sector de grandes empresas

Por tercer año consecutivo, las grandes empresas señalaron la **explotación de vulnerabilidades** como la principal causa raíz de los ataques de ransomware, representando un 29 % de los incidentes. Los **correos de phishing** ocuparon el segundo lugar, pasando del 11 % en 2024 al 21 % en 2025.

Los **ataques basados en credenciales** siguen representando un riesgo significativo, si bien su incidencia se ha reducido considerablemente, pasando del 30 % en 2024 al 21 % en 2025. Por contra, según las **pequeñas y medianas empresas** (aquellas con entre 100 y 250 empleados), los ataques basados en credenciales son la principal causa raíz de los ataques de ransomware, responsables de casi un tercio (30 %) de los incidentes.

Gráfico 1: causa raíz técnica de los ataques de ransomware en las grandes empresas 2023 - 2025

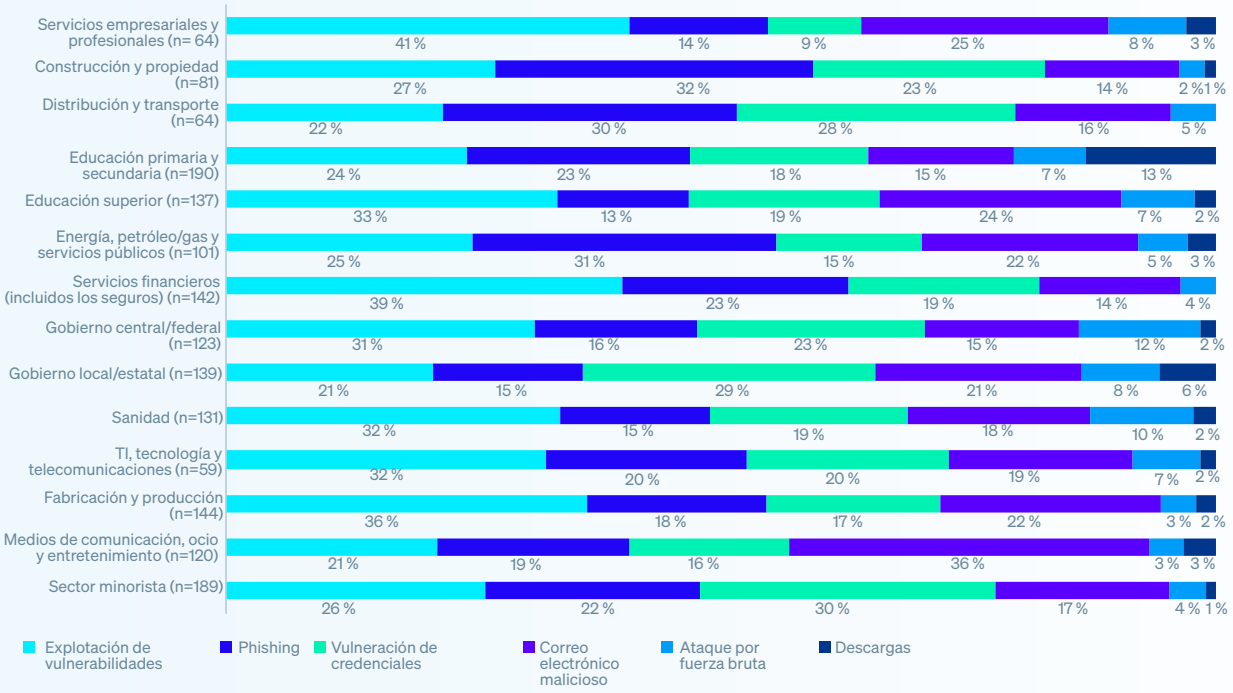


¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? - Sí. n=1733 (2025), 1409 (2024), 1045 (2023).

La investigación revela que, a pesar de que las causas raíz varían en función del sector, la explotación de vulnerabilidades es un vector importante para las grandes empresas de casi todos los sectores. Excepciones importantes:

- El **phishing** fue la causa raíz más común citada tanto por los sectores de **construcción y propiedad** (32 %), **distribución y transporte** (30 %) y **energía, petróleo/gas y servicios públicos** (31 %).
- La **vulneración de credenciales** fue el vector de ataque percibido más común por las grandes empresas del **sector minorista**, representando casi un tercio de los incidentes (30 %).

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

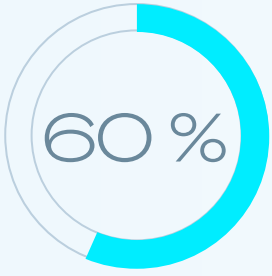


¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? - Sí. Números base en la tabla.

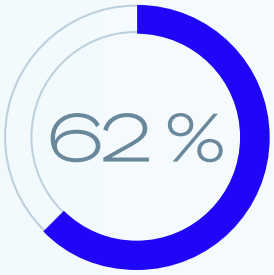
Causa raíz organizativa de los incidentes en el sector de grandes empresas

Además de las causas técnicas de los incidentes, también es importante comprender los factores organizativos que exponen a las grandes empresas a los ataques. Los resultados revelan que las víctimas del sector de grandes empresas suelen enfrentarse a múltiples retos organizativos: de media, los encuestados citaron tres factores que contribuyeron a sufrir un ataque de ransomware.

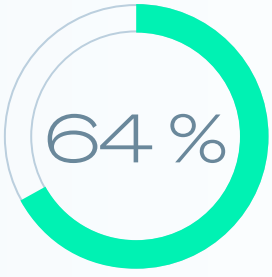
En general, las causas raíz organizativas están repartidas de forma muy equilibrada entre problemas de protección, problemas de recursos y lagunas de seguridad. Sin embargo, las grandes empresas tienden un poco más a citar las lagunas de seguridad (conocidas y desconocidas) como factor principal.



FALTA DE PROTECCIÓN O PROTECCIÓN DEFICIENTE
Falta de protección o soluciones de protección deficientes que no pudieron detener el ataque



FALTA DE PERSONAL/ CONOCIMIENTOS TÉCNICOS
La falta de experiencia humana (habilidades o capacidad) necesaria para detectar y detener el ataque a tiempo



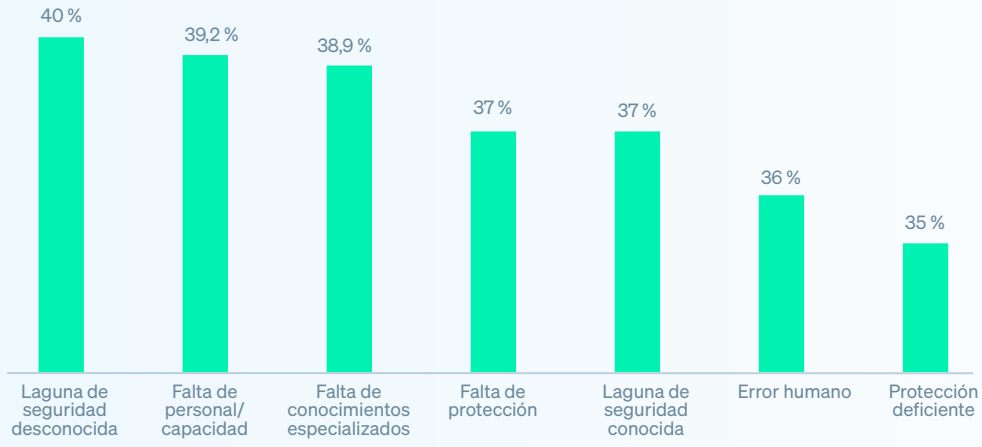
LAGUNA DE SEGURIDAD (CONOCIDA O DESCONOCIDA)
Tenían debilidades conocidas o desconocidas en sus defensas

¿Por qué cree que su organización sufrió un ataque de ransomware? n=1733. Respuestas consolidadas.

Las **lagunas de seguridad desconocidas** (es decir, debilidades en las defensas que los encuestados desconocían) es la razón individual más común, nombrada por el 40 % de los encuestados del sector de grandes empresas. Les siguen de cerca 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) y la **falta de conocimientos especializados** (es decir, no disponer de las habilidades o los conocimientos necesarios para detectar y detener el ataque a tiempo), factores que el 39 % de las grandes empresas identificaron como determinantes.

Curiosamente, las **pymes** también señalaron la **falta de personal/capacidad** como un factor común, y el 42 % la citó como una de las razones principales de haber sido víctimas, lo que pone de relieve que la escasez de recursos sigue siendo un problema generalizado, independientemente del tamaño de la organización.

Gráfico 3: causa raíz operativa de los ataques de ransomware en grandes empresas



¿Por qué cree que su organización sufrió un ataque de ransomware? n=1733.

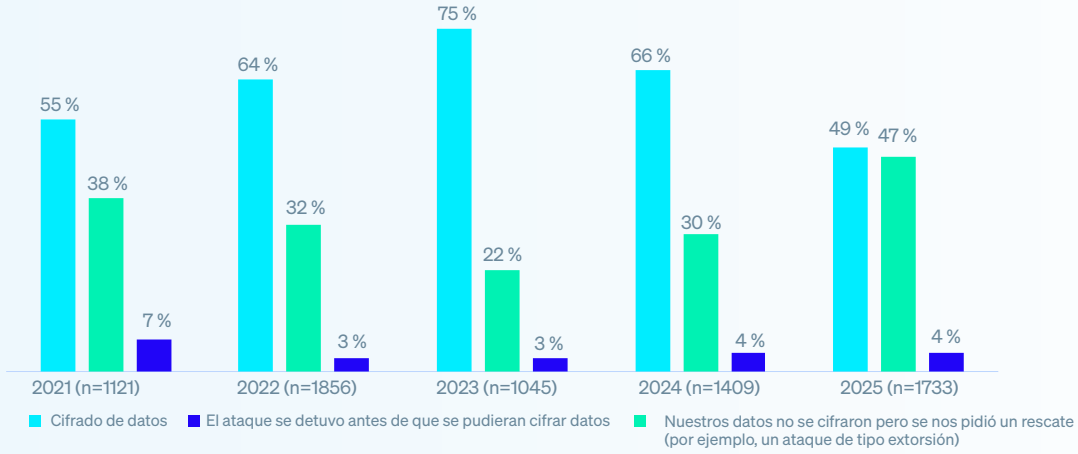
Qué ocurre con los datos

Cifrado de datos en el sector de grandes empresas

Es alentador que el índice de cifrado de datos en las grandes empresas se sitúe en su nivel más bajo en los cinco años que llevamos realizando este estudio: menos de la mitad (49 %) de los ataques se saldaron con el cifrado de datos, frente al 66 % registrado en 2024.

Por otra parte, el porcentaje de ataques de ransomware detenidos antes del cifrado de datos se ha duplicado con creces en los últimos dos años, pasando del 22 % en 2023 al 47 % en 2025. Esto sugiere que las grandes empresas están siendo cada vez más eficaces a la hora de detectar y detener los ataques antes de que causen daños graves.

Gráfico 4: índice de cifrado de datos en los ataques de ransomware a grandes empresas 2021 - 2025

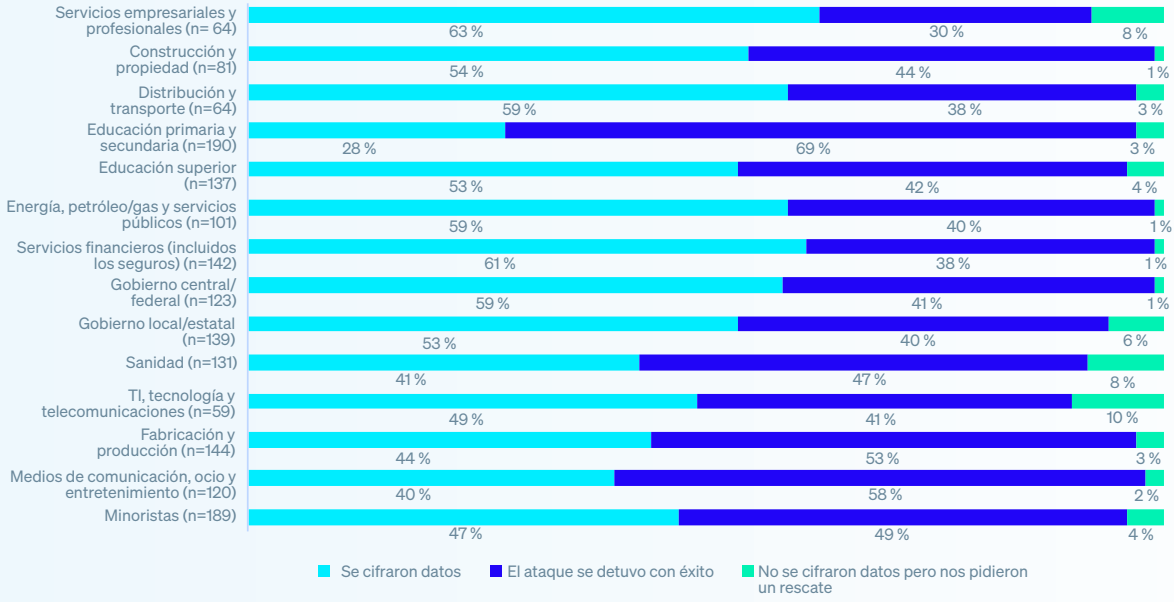


¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Números base en la tabla.

Índice de cifrado de datos por sector

Las grandes empresas del sector de los **servicios empresariales y profesionales** son las más propensas a sufrir el cifrado de datos (63 %), lo que indica que la organizaciones de este sector tienen mayores dificultades para detectar y detener el ataque antes del cifrado 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 28 %.

Gráfico 5: índice de cifrado de datos en grandes empresas por sector



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

Robo de datos

Los adversarios no solo cifran los datos, sino que también los roban. Entre las grandes empresas, el 15 % de todas las víctimas de ransomware y el 30 % de las organizaciones cuyos datos fueron cifrados sufrieron además el robo de datos. Si analizamos los datos por sector vemos que:

- En el extremo superior, el 52 % de las grandes empresas del sector de los **medios de comunicación, ocio y entretenimiento** cuyos datos fueron cifrados también sufrieron el robo de datos.
- Por el contrario, solo el 11 % de las grandes empresas del sector de la **construcción y la propiedad** sufrieron el robo de datos además del cifrado.

Ataques de tipo extorsión

Como se muestra en el gráfico 4, la proporción de grandes empresas que evitaron el cifrado de datos pero que aún así se les pidió un rescate se ha mantenido estable año tras año en un 4 %. Si lo desglosamos por sector, las organizaciones de **TI, tecnología y telecomunicaciones** fueron las más expuestas a este tipo de ataques, con un índice del 10 %, mientras que las grandes empresas de los sectores de **construcción y propiedad, energía, petróleo/gas y servicios públicos, servicios financieros y gobierno central/federal** fueron las menos afectadas, ya que solo registraron un 1 %.

En general, las grandes empresas del sector de la **educación primaria y secundaria** son las que mejor pueden prevenir 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 tempranas, incluso con presupuestos limitados.

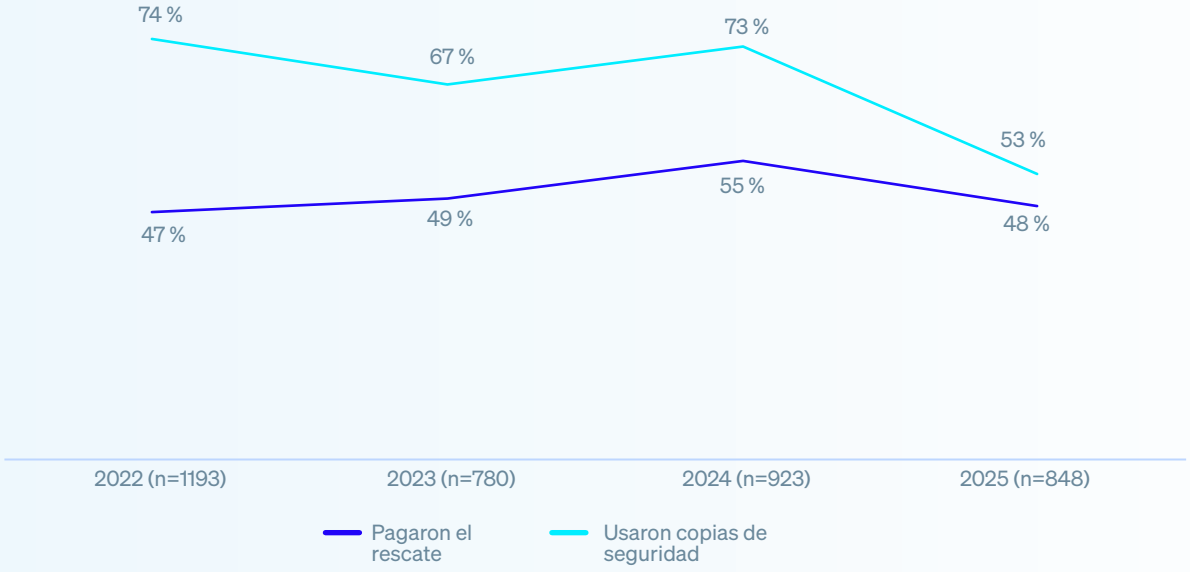
Recuperación de los datos cifrados en el sector de grandes empresas

El 96 % de las grandes empresas a las que les cifraron los datos pudieron recuperarlos.

En 2025, el 48 % de las grandes empresas **pagaron el rescate para recuperar sus datos**, lo que supone un descenso con respecto al 55 % de 2024. Al mismo tiempo, el **uso de copias de seguridad** se redujo drásticamente hasta alcanzar su nivel más bajo en cuatro años (53 %, frente al 73 % de 2024). En conjunto, estas conclusiones apuntan a una mayor resistencia frente a las peticiones, así como a debilidades y a una falta de resiliencia a la hora de realizar copias de seguridad.

Además, la reducción de la brecha entre las grandes empresas 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. Como prueba de ello, comprobamos que casi un tercio (30 %) de las grandes empresas cuyos datos fueron cifrados afirmaron **haber utilizado otros métodos para restaurarlos**. Entre los métodos alternativos se incluyen la restauración a partir de instantáneas, el uso de funciones de reversión de la protección para endpoints o la recuperación de datos de sistemas no afectados.

Gráfico 6: recuperación de los datos cifrados en las grandes empresas 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 de grandes empresas

En el último año, la mediana de petición de rescate para las grandes empresas se ha desplomado un 56 %, pasando de 2,75 millones USD en 2024 a 1,20 millones USD en 2025. El descenso de las peticiones de rescate dirigidas a este sector obedece en gran medida a una reducción del 24 % en las peticiones de 5 millones USD o más durante el último año. No obstante, es importante señalar que las peticiones de rescate por valor de 1 a 5 millones USD aumentaron un 17 %, lo que representa el 27 % del total, frente al 23 % registrado en 2024.

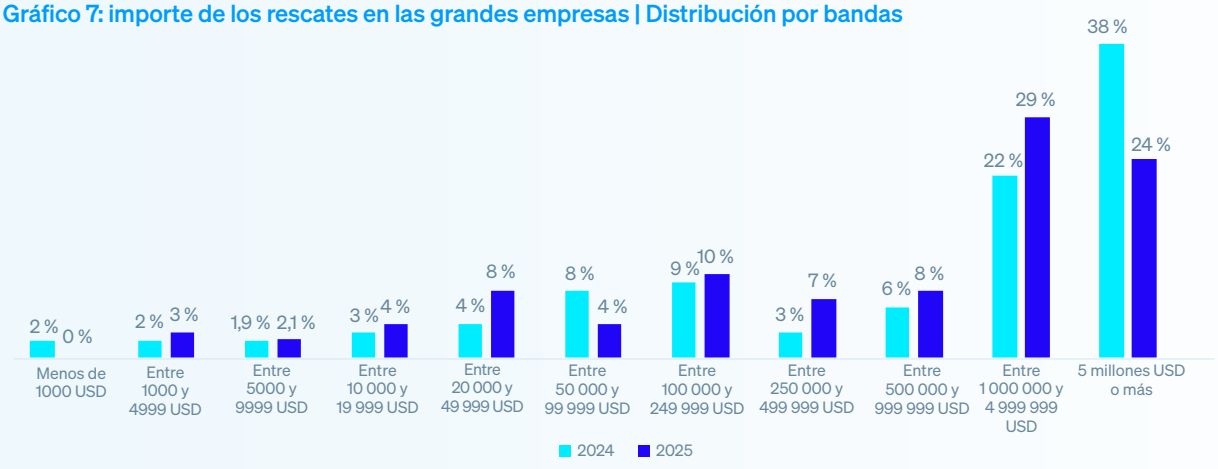
Importes de los rescates en el sector de grandes empresas

Siguiendo esta tendencia, la mediana del rescate pagado por las grandes empresas también disminuyó, pasando de 1,26 millones USD en 2024 a solo 1 millón USD en 2025. La caída se debe en gran medida a un descenso del 37 % en los pagos de 5 millones USD o más en el último año. Sin embargo, el informe pone de manifiesto aumentos interanuales en casi todas las franjas de pagos inferiores a 5 millones USD.

Estos patrones sugieren que los atacantes están dejando de pedir grandes rescates y, en su lugar, se dirigen a las grandes empresas con exigencias más modestas, con el objetivo de conseguir cantidades que sigan siendo importantes, pero que puedan pagarse de forma más realista.

Las **pymes** siguieron un patrón similar, aunque la caída de las peticiones de rescates y los pagos ha sido aún más pronunciada. La mediana de las peticiones e importes de los rescates descendió bruscamente de 2 millones USD en 2024 a 126 000 USD y 200 000 USD en 2025, respectivamente, lo que confirma la tendencia general de los atacantes a recalibrar sus expectativas hacia sumas más asequibles en organizaciones de todos los tamaños.

Gráfico 7: importe de los rescates en las grandes empresas | Distribución por bandas

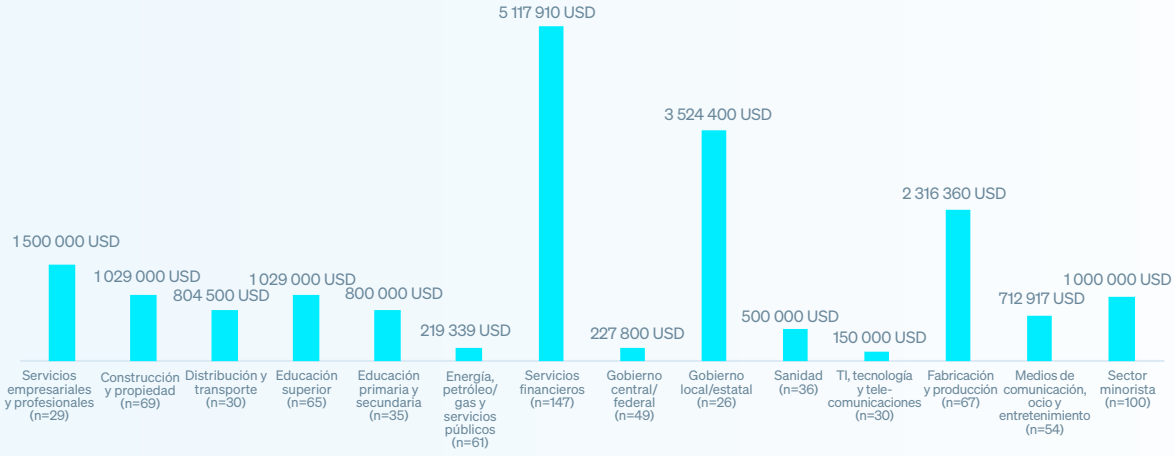


¿Cuál fue el importe de rescate que pagó su organización a los atacantes? n=414 (2025), 470 (2024)

Importes de los rescates por sector

Los importes de los rescates variaron considerablemente dependiendo del sector, siendo las grandes empresas las que pagaron el importe medio más alto (mediana) a los atacantes: 5,1 millones USD. Esto puede deberse a que el sector se juega mucho en el terreno operativo y tiene poca tolerancia a las interrupciones, algo que lleva a los atacantes a pensar que los pagos más elevados tienen más probabilidades de ser tenidos en cuenta.

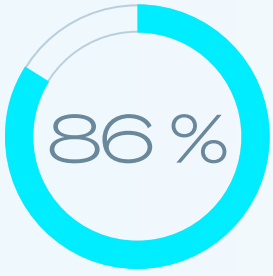
Gráfico 8: Importes de los rescates por sector



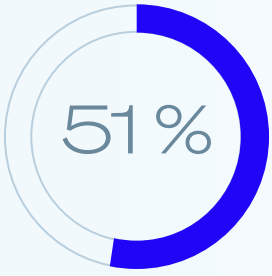
¿A cuánto ascendió el rescate que pagó su organización a los atacantes? Números base en la tabla. Nota: cuando los números base son inferiores a 30, los resultados deben considerarse meramente indicativos.

Comparativa entre los importes desembolsados por las grandes empresas y la petición inicial

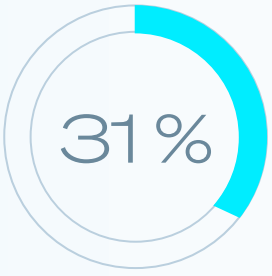
414 grandes empresas que pagaron el rescate compartieron tanto la petición inicial como la cantidad pagada realmente, lo que puso de manifiesto que pagaron, de media, el 86 % de la petición de rescate inicial, un bienvenido descenso con respecto al 95 % registrado en 2024. En general, el 51 % pagó menos de lo que se pedía inicialmente, el 18 % pagó más y cerca de un tercio (31 %) igualó la petición inicial.



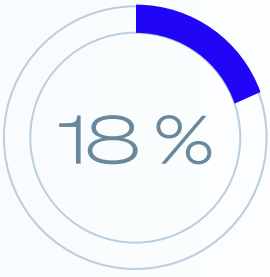
porcentaje **que se pagó** de la petición de rescate, de media



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

Por qué la mayoría de los importes de rescate pagados por las grandes empresas difieren del importe exigido inicialmente

La encuesta también explora por qué algunas grandes empresas 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 72 grandes empresas que **pagaron más** que la petición inicial:

- 61 %: Los atacantes creían que podíamos permitirnos pagar más.
- 49 %: Los adversarios se dieron cuenta de que somos un objetivo valioso.
- 42 %: Nuestras copias de seguridad fallaron o no funcionaron bien.
- 39 %: Los atacantes se frustraron y aumentaron el precio.
- 31 %: No pagamos lo bastante rápido, así que subió el precio.

Por lo general, las grandes empresas 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.

214 grandes empresas que **pagaron menos** que la petición inicial explicaron cómo consiguieron reducir el importe del rescate:

- 49 %: Negociamos una cantidad inferior con los atacantes.
- 46 %: Nos hicieron un descuento por pagar el rescate rápido.
- 45 %: Los atacantes rebajaron su petición para animarnos a pagar.
- 43 %: Los atacantes redujeron su petición inicial debido a presiones externas (por ejemplo, de los medios de comunicación o de las fuerzas de seguridad).
- 38 %: 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 sector de grandes empresas

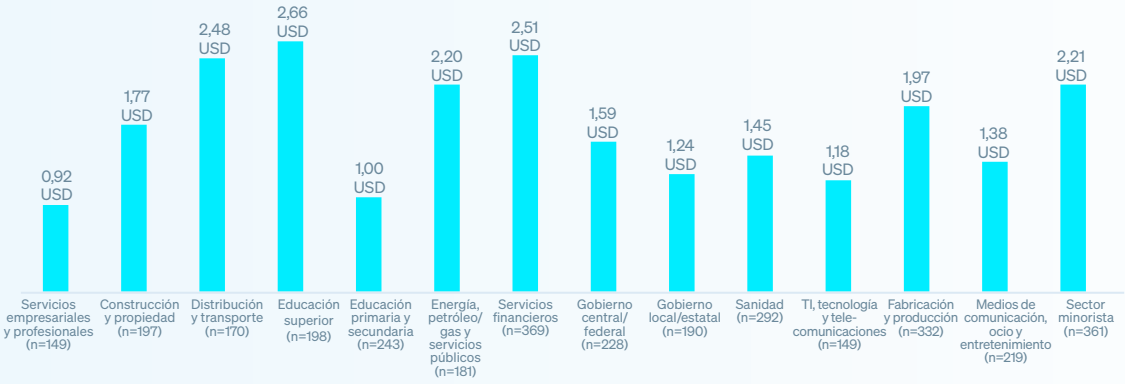
En el último año, el coste medio para las grandes empresas de recuperarse de un ataque de ransomware (sin contar el pago del rescate) ha caído a su punto más bajo en tres años, con un descenso del 41 % en el último año, hasta 1,84 millones USD, por debajo de los 3,12 millones USD de 2024. También es 330 000 USD inferior a los 2,17 millones USD registrados en 2023.

2023	2024	2025
2,17 MUSD	3,12 MUSD	1,84 MUSD

¿Cuál fue el coste aproximado, sin incluir el pago de rescates, que tuvo que asumir la 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=1.733 (2025), 1.409 (2024), 1.045 (2023)

Al analizar el desglose por sector, el importe de la recuperación varía notablemente. Las grandes empresas del sector de **educación primaria y secundaria** registraron el coste medio más alto para rectificar incidentes: 2,66 millones USD. En cambio, las grandes empresas del sector de los **servicios empresariales y profesionales** registraron el coste más bajo: 0,92 millones USD. Es probable que esta diferencia refleje en parte el diferente nivel de reconstrucción de la infraestructura de TI necesaria para recuperarse del ataque, ya que las organizaciones de educación primaria y secundaria suelen utilizar soluciones más antiguas que los proveedores de servicios del sector privado.

Gráfico 9: coste de recuperación del ransomware por sector (millones de USD)

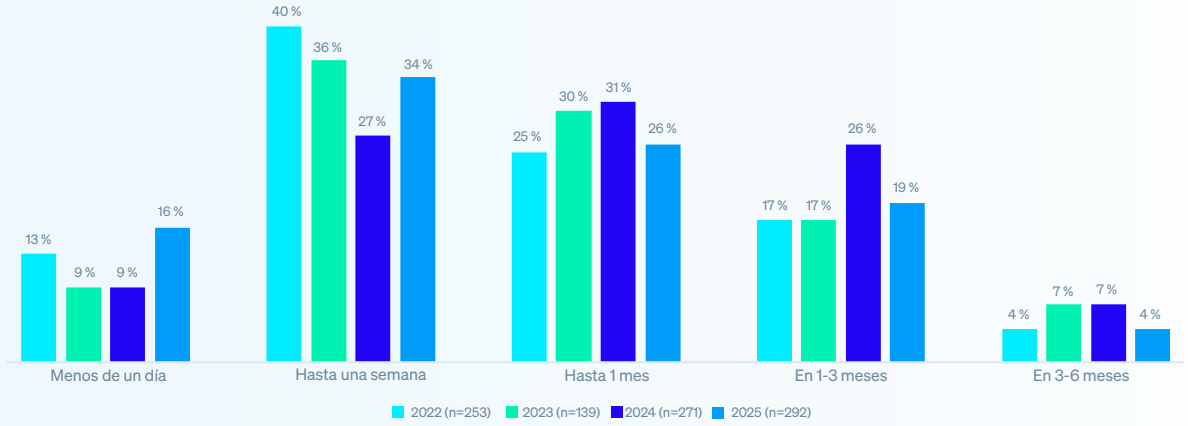


¿Cuál fue el coste aproximado que tuvo que asumir su organización para rectificar los perjuicios del ataque de ransomware más significativo (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, etc.)? Números base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

Tiempo de recuperación en el sector de grandes empresas

Los datos ponen de manifiesto que, en 2025, las grandes empresas se recuperan más rápidamente de los ataques de ransomware. La mitad se recuperó en una semana, frente al 36 % de 2024. Además, la proporción de organizaciones a las que les cuesta recuperarse de uno a tres meses descendió al 19 %, frente al 26 % de 2024. En general, el 95 % de las grandes empresas afectadas se recuperaron completamente en menos de tres meses, lo que pone de relieve la creciente resiliencia y capacidad de recuperación de todo el sector.

Gráfico 10: tiempo de recuperación para las grandes empresas tras ataques de ransomware 2022 - 2025

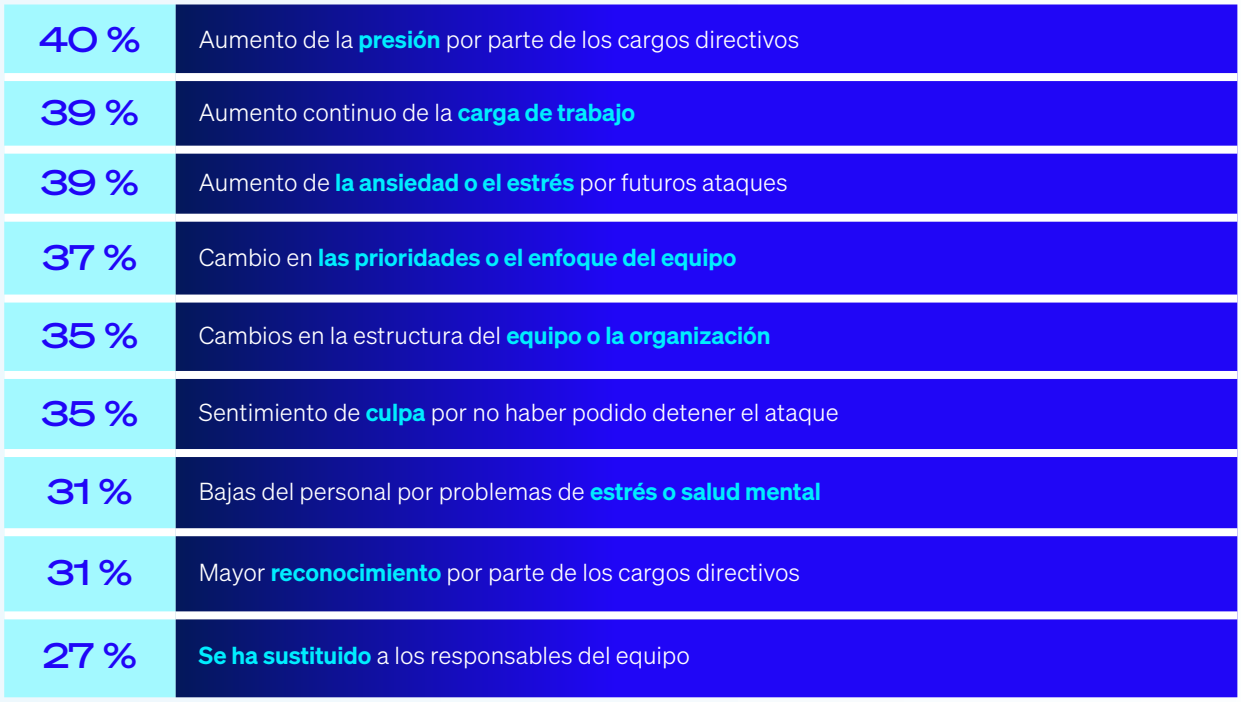


¿Cuánto tiempo tardó su organización en recuperarse totalmente del ataque de ransomware? Números base en la tabla.

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 de grandes empresas, ya que todos los encuestados afirman que sus equipos se han 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=848

Recomendaciones

Aunque las grandes empresas han percibido varios cambios con respecto al ransomware durante el último año, este sigue siendo una importante amenaza. A medida que los adversarios continúan 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. 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 empresa.

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 funciones next-gen probadas, los datos de su empresa estarán protegidos de forma eficaz por productos basados en la IA y el Machine Learning.

2025-12-08 WP (MP)

SOPHOS