

SOPHOS

# EL ESTADO DEL RANSOMWARE EN MÉXICO 2025

Resultados de una encuesta independiente desvinculada de cualquier proveedor a 111 organizaciones en México que se vieron afectadas por el ransomware en el último año.

# Acerca del informe

Los resultados se basan en una encuesta independiente y desvinculada de cualquier proveedor realizada a 3400 responsables de TI/ ciberseguridad que trabajan en organizaciones que se vieron afectadas por el ransomware en el último año, entre ellas 111 de México.

La encuesta fue 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.

El informe recoge comparaciones con los resultados de nuestra encuesta de 2024. Todos los puntos de datos financieros son en dólares estadounidenses (USD).

Encuesta a

111

responsables de TI/ciberseguridad en México en organizaciones que se vieron afectadas por el ransomware en el último año



Porcentaje de ataques que comportaron el cifrado de datos.



La causa raíz técnica más común de los ataques.



Coste medio de recuperación de un ataque de ransomware.

## Por qué sucumben las organizaciones mexicanas al ransomware

- ▶ **La explotación de vulnerabilidades fue la causa raíz técnica más común de los ataques**, utilizada en el 45 % de los incidentes. Le sigue el compromiso de credenciales, que originó el 28 % de los ataques. Los correos maliciosos se utilizaron en el 13 % de los ataques.
- ▶ **Una laguna de seguridad conocida fue la causa raíz operativa más común**, mencionada por el 47 % de los encuestados en México. Le siguió una laguna de seguridad desconocida, que fue citada por el 43 % de las organizaciones. Según el 40 %, el hecho de no disponer de las habilidades o los conocimientos necesarios para detectar y detener el ataque a tiempo influyó en que su organización sufriera un ataque de ransomware.

## Qué ocurre con los datos

- ▶ **El 50 % de los ataques comportaron el cifrado de datos**, lo que coincide con la media mundial.
- ▶ **También se robaron datos en el 52 % de los ataques en que se cifraron datos.**
- ▶ **Todas las organizaciones mexicanas a las que les cifraron los datos pudieron recuperarlos**, por encima de la media global.
- ▶ **El 23 % de las organizaciones mexicanas pagaron el rescate y recuperaron los datos**, muy por debajo de la media mundial del 49 %.
- ▶ **El 68 % de las organizaciones mexicanas utilizaron copias de seguridad para recuperar los datos cifrados.**

## Los rescates: peticiones e importes

- ▶ **La mediana de petición de rescate en México el año pasado fue de dos millones USD**, muy por encima de la media global de 1,32 millones USD.



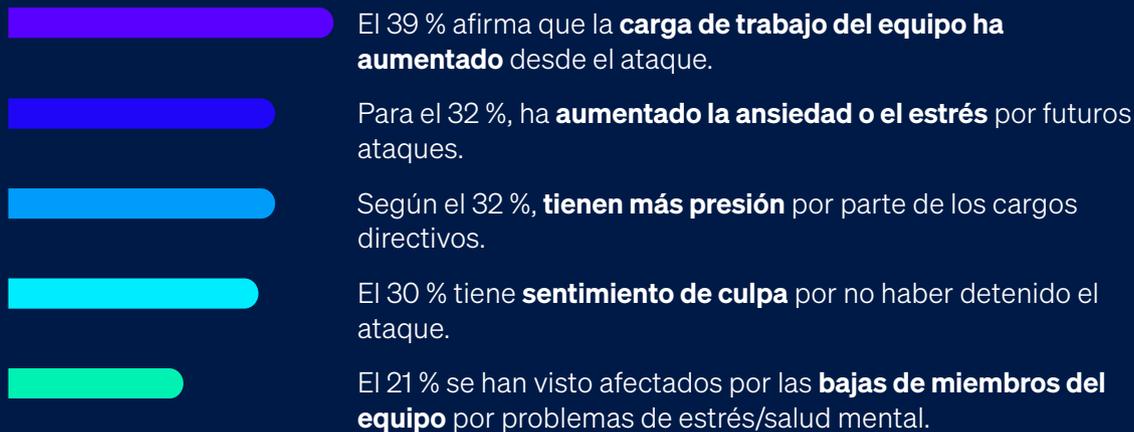
Mediana del importe de rescate en México el año pasado.

- ▶ **Cerca de tres cuartas partes (70 %) de las peticiones de rescate ascendieron a 1 millón USD o más.**
- ▶ 13 encuestados de México cuya organización pagó el rescate compartieron la cantidad: **la mediana del importe de rescate fue 1 millón USD.**
- ▶ **Por lo general, las organizaciones mexicanas suelen pagar TODO el rescate exigido**, muy por encima de la media mundial del 85 %.
  - El 46 % **pagó MENOS de lo que se pedía inicialmente** por el rescate (media global: 53 %).
  - El 23 % **IGUALÓ la petición inicial** (media global: 29 %).
  - El 31 % **pagó MÁS de lo que se pedía inicialmente** (media global: 18 %).

## El impacto del ransomware en el negocio

- ▶ Excluyendo los pagos de rescates, **la factura media en la que incurrieron las organizaciones mexicanas para recuperarse de un ataque de ransomware el año pasado fue de 1,35 millones USD**, muy por debajo de la media global de 1,53 millones USD. Incluye los costes de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, etc.
- ▶ **Las organizaciones mexicanas se recuperan rápidamente de los ataques de ransomware:** el 64 % se recuperó totalmente en menos de una semana (muy por encima de la media mundial del 53 %) y solo el 10 % tardó entre uno y seis meses en recuperarse.

## El impacto del ransomware a nivel humano en los equipos de TI/ ciberseguridad de las organizaciones cuyos datos fueron cifrados



## Recomendaciones

El ransomware sigue siendo una amenaza importante para las organizaciones mexicanas. 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. Las conclusiones de este informe nos indican en qué áreas debemos centrarnos en 2025 y más allá.

- ▶ **Prevención.** El mejor ataque de ransomware es aquel que no se llega a producir porque los adversarios no consiguen entrar en su organización. Trate de reducir las causas raíz de los ataques, tanto técnicas como operativas, que se destacan aquí.
- ▶ **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.
- ▶ **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.
- ▶ **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.

# SOPHOS

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

[es.sophos.com/ransomware2025](https://es.sophos.com/ransomware2025)

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.