SOPHOS

EL ESTADO DEL RANSOMWARE EN COLOMBIA 2025

Resultados de una encuesta independiente desvinculada de cualquier proveedor a 122 organizaciones en que se vieron afectadas por el ransomware en Colombia el último año.

MONOGRÁFICOS DE SOPHOS - JUNIO DE 2025

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 122 de Colombia.

La encuesta fue encargada por Sophos y realizada por un especialista externo entre enero y marzo de 2025.

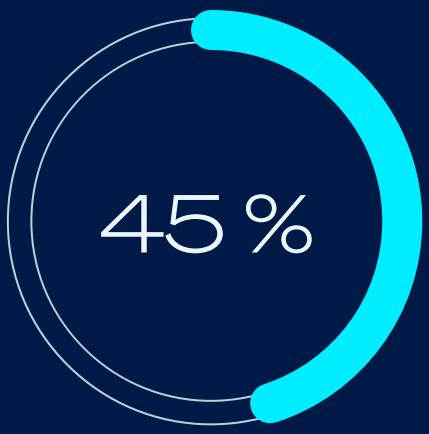
Todos los encuestados trabajan en organizaciones con entre 100 y 5000 empleados, y se les pidió contestar según sus experiencias en los últimos 12 meses.

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

122

responsables de TI/ciberseguridad en Colombia 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 colombianas al ransomware

- **La explotación de vulnerabilidades fue la causa raíz técnica más común de los ataques**, utilizada en el 30 % de los incidentes. Le sigue el compromiso de credenciales, que originó el 27 % de los ataques. Los correos maliciosos se utilizaron en el 24 % de los ataques.
- Las **lagunas de seguridad conocidas** y la **falta de conocimientos especializados fueron las dos causas raíz operativas más comunes**, ambas citadas por el 43 % de los encuestados colombianos. Según el 41 %, el hecho de no disponer de los productos y servicios de ciberseguridad necesarios influyó en que su organización sufriera un ataque de ransomware.

Qué ocurre con los datos

- **El 45% de los ataques comportaron el cifrado de datos.** Esto es algo inferior a la media global (50 %).
- **También se robaron datos en el 18 % de los ataques en que se cifraron datos.**
- **El 98 % de las organizaciones colombianas a las que les cifraron los datos pudieron recuperarlos.**
- **El 18 % de las organizaciones colombianas pagaron el rescate y recuperaron los datos,** un porcentaje muy inferior al 49 % de la media mundial.
- **El 56 % de las organizaciones colombianas utilizaron copias de seguridad para recuperar los datos cifrados.**

Los rescates: peticiones e importes

- 24 encuestados de Colombia cuyos datos fueron cifrados compartieron el importe de rescate que los atacantes les exigieron inicialmente: la **mediana de petición de rescate en el último año fue de 60 000 USD**.

Mediana del importe de rescate en Colombia el año pasado.

- **El 63 % de las peticiones de rescate ascendieron a cantidades de hasta 99 999 USD.**
- Diez encuestados de Colombia cuya organización pagó el rescate compartieron la cantidad: **la mediana del importe de rescate fue 40 000 USD**.
- **Por lo general, las organizaciones colombianas pagaron el 78 % de la petición de rescate**, por debajo de la media mundial del 85 %.
  - El 70 % **pagó MENOS de lo que se pedía inicialmente** por el rescate (media global: 53 %).
  - El 20 % **IGUALÓ la petición inicial** (media global: 29 %).
  - El 10 % **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 chilenas para recuperarse de un ataque de ransomware el año pasado fue de 0,87 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 colombianas se recuperan rápidamente de los ataques de ransomware:** el 50 % se recuperó totalmente en menos de una semana, justo por debajo de la media mundial del 53 %. El 25 % 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

El 45 % se han visto afectados por las **bajas de miembros del equipo** por problemas de estrés/salud mental.

El 44 % tiene **sentimiento de culpa** por no haber detenido el ataque.

El 33 % afirma que la **carga de trabajo del equipo ha aumentado** desde el ataque.

Para el 29 %, ha **aumentado la ansiedad o el estrés** por futuros ataques.

Según el 24 %, **tienen más presión** por parte de los cargos directivos.

Recomendaciones

El ransomware sigue siendo una amenaza importante para las organizaciones colombianas. 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.
- **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.

SOPHOS

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

2025-07-10 CO-WP (DD)