SOPHOS

EL ESTADO DEL RANSOMWARE EN COLOMBIA 2026

Resultados de una encuesta independiente desvinculada de cualquier proveedor a 49 organizaciones en Colombia que se vieron afectadas por el ransomware en el último año.

MONOGRÁFICOS DE SOPHOS - JULIO DE 2026

Acerca del informe

Este séptimo informe anual sobre el estado del ransomware se basa en los resultados de una encuesta independiente encargada por Sophos. El informe global de este año se basa en las experiencias de 2158 responsables de TI y ciberseguridad que trabajan en organizaciones que se vieron afectadas por el ransomware en el último año, entre ellas 49 de Colombia.

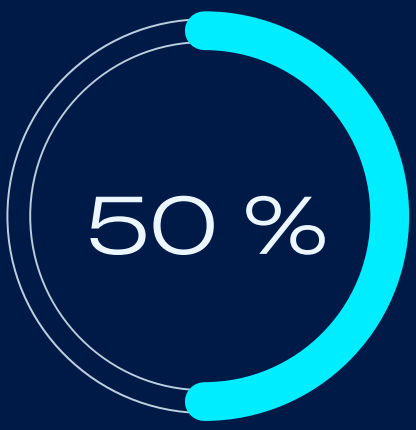
La encuesta se realizó entre enero y marzo de 2026. Todos los encuestados trabajan en organizaciones con entre 100 y 5000 empleados, y se les pidió contestar según sus experiencias en los últimos 12 meses. Todos los puntos de datos financieros son en dólares estadounidenses (USD). Se han eliminado de estos datos los rescates atípicos de 40 millones USD o más.

Encuesta a

49

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

La causa raíz técnica más común de los ataques.



Confirmaron que el incidente de ransomware del año pasado fue el mismo que el ataque de identidad más significativo.

Coste medio de recuperación de un ataque de ransomware.

Por qué sucumben las organizaciones colombianas al ransomware

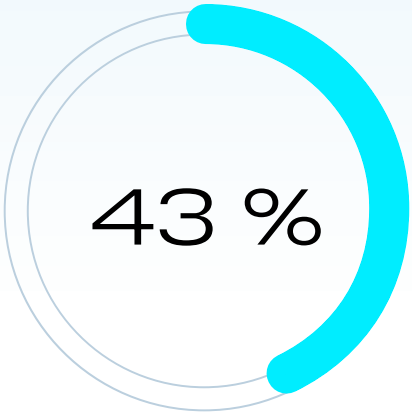
- **Los correos electrónicos maliciosos fueron la causa raíz técnica más frecuente de los ataques,** ya que se utilizaron en el 33 % de los mismos, seguidos del compromiso de credenciales (29 %) y del phishing (18 %). La explotación de vulnerabilidades disminuyó drásticamente, situándose en el 4 %, frente al 30 % registrado en el informe de 2025.
- **La falta de protección (45 %) fue la causa raíz operativa más común,** seguida de una laguna de seguridad conocida (41 %) y del error humano (37 %).
- **(NOVEDAD) El 50 % confirmó que el incidente de ransomware del año pasado coincidió con su ataque más significativo relacionado con la identidad.**

El impacto del ransomware en el negocio

- Sin tener en cuenta los pagos de rescate, **el coste medio de recuperación para las organizaciones colombianas fue de 650 510 USD,** lo que supone un descenso notable con respecto a la media de 872 377 USD registrada en el informe de 2025. Incluye los costes de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, etc.
- **El 78 % de las organizaciones colombianas se recuperó de un ataque de ransomware en un plazo inferior a una semana,** lo que supone un aumento considerable con respecto al 50 % registrado en 2025. El 4 % tardó entre uno y seis meses en recuperarse, un descenso considerable con respecto al 25 % registrado en la edición del informe de 2025.

Qué ocurre con los datos

- **El 43 % de los ataques comportaron el cifrado de datos.** Esta cifra es inferior a la media mundial del 56 % y supone un descenso con respecto al 45 % registrado por los encuestados colombianos en 2025.



de los ataques comportaron el cifrado de datos

Recomendaciones

Refuerce la seguridad de la identidad como medida de defensa contra el ransomware. Aproximadamente la mitad de las víctimas de ransomware en Colombia confirmaron que su incidente de ransomware coincidió con su ataque más grave relacionado con la identidad, lo que pone de relieve el estrecho vínculo que existe entre la vulneración de la identidad y el ransomware. Las organizaciones deben priorizar la detección y respuesta ante amenazas relacionadas con la identidad (ITDR), aplicar la autenticación multifactor en todos los puntos de acceso y auditar periódicamente las credenciales de identidad, tanto humanas como no humanas. Tal y como puso de manifiesto el informe global (el 97 % de las organizaciones había habilitado la MFA en el momento del ataque), la MFA por sí sola no es suficiente para detener los ataques, por lo que es necesario implementarla de forma integral.

Refuerce la protección para endpoints frente a los modelos de IA de frontera. La IA de vanguardia está acelerando el descubrimiento de vulnerabilidades y la posibilidad de explotarlas. Es fundamental contar con defensas sólidas en los endpoints que bloqueen automáticamente los ataques basados en exploits.

Priorice la seguridad del correo electrónico. Dado que el phishing y los correos electrónicos maliciosos representan casi la mitad de las causas raíz de los ataques de ransomware en Colombia, las organizaciones deben implementar un filtrado avanzado del correo electrónico, aplicar los protocolos DMARC/DKIM/SPF e invertir en formación periódica sobre concienciación frente al phishing.

Invierta en infraestructura de copias de seguridad y recuperación. El año pasado, las organizaciones que contaban con sistemas de copias de seguridad sólidos recuperaron los datos cifrados a un ritmo casi sin precedentes. Las copias de seguridad deben someterse a pruebas periódicas, almacenarse fuera de línea o en formatos inmutables e integrarse en un plan de respuesta ante incidentes documentado que pueda ejecutarse en situaciones de presión.

Para descubrir cómo Sophos puede ayudarle a optimizar sus defensas contra el ransomware, hable con un asesor o visite **es.sophos.com/ransomware2026**.

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.

2026-08-03 CO-WP (TA) CRE-6005