SOPHOS

EL ESTADO DEL RANSOMWARE EN CHILE 2026

Resultados de una encuesta independiente desvinculada de cualquier proveedor a 48 organizaciones en Chile 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 48 de Chile.

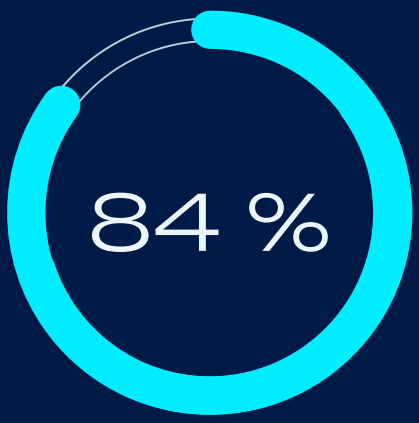
La encuesta se realizó entre enero y marzo de 2026. Todos los encuestados trabajan en organizaciones con entre 100 y 5000 empleados, y se les pidió contestar según sus experiencias en los últimos 12 meses. Todos los puntos de datos financieros son en dólares estadounidenses (USD). Se han eliminado de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

Encuesta a

48

responsables de TI/ciberseguridad en Chile 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 chilenas al ransomware

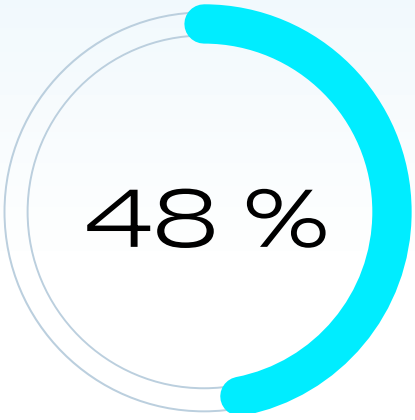
- **La explotación de vulnerabilidades fue la causa raíz técnica más común de los ataques,** utilizada en el 33 % de los incidentes. Le siguieron los correos electrónicos maliciosos, origen del 31 % de los ataques. En el 21 % de los ataques, se recurrió al compromiso de credenciales. La explotación de vulnerabilidades disminuyó drásticamente, situándose en el 33 %, frente al 46 % registrado en el informe de 2025.
- **La falta de conocimientos especializados (52 %) fue la causa raíz operativa más común,** seguida de una laguna de seguridad desconocida (48 %) y de la falta de personal/capacidad (48 %).
- **(NOVEDAD) Los dispositivos de los usuarios fueron el punto de entrada más habitual (52 %)** en los casos de relacionados con la explotación de vulnerabilidades, el compromiso de credenciales y los ataques por fuerza bruta. Las aplicaciones y los sistemas expuestos (32 %) y los firewalls (13 %) ocuparon el segundo y tercer lugar, respectivamente.
- **(NOVEDAD) El 84 % confirmó que el incidente de ransomware del año pasado coincidió con su ataque más significativo relacionado con la identidad.** Aunque no todos los ataques dieron lugar al cifrado de datos, esto confirma que el robo de identidad es uno de los principales mecanismos de distribución del ransomware.

El impacto del ransomware en el negocio

- Sin tener en cuenta los pagos de rescate, **el coste medio de recuperación para las organizaciones chilenas fue de 1,04 millones USD,** lo que supone un ligero descenso con respecto a la media de 1,2 millones USD que figuraba 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 44 % de las organizaciones chilenas se recuperó de un ataque de ransomware en un plazo inferior a una semana,** lo que supone una reducción significativa con respecto al 65 % registrado en 2025. El 21 % tardó entre uno y seis meses en recuperarse, un aumento considerable con respecto al 8 % registrado en la edición del informe de 2025.

Qué ocurre con los datos

- **El 48 % 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 52 % registrado por los encuestados chilenos en 2025.



de los ataques comportaron el cifrado de datos.

Recomendaciones

Refuerce la seguridad de la identidad como medida de defensa contra el ransomware. La gran mayoría de las víctimas de ransomware en Chile confirmaron que el incidente que sufrieron coincidió con su ataque más significativo relacionado con la identidad. 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.

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 un tercio de las causas raíz de los ataques de ransomware en Chile, 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.

SOPHOS

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.

2026-07-28 CL-WP (TA) CRE-6013