SOPHOS

EL ESTADO DEL RANSOMWARE EN CHILE 2025

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

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

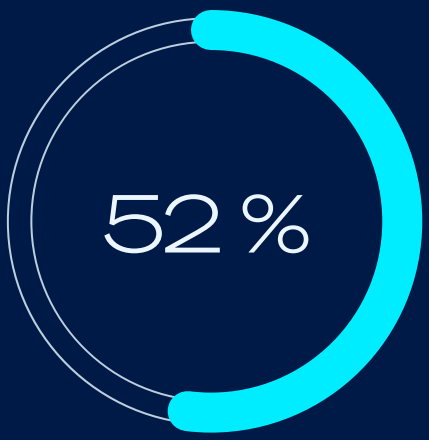
Todos los encuestados trabajan en organizaciones con entre 100 y 5000 empleados, y se les pidió contestar según sus experiencias en los últimos 12 meses.

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 Chile en organizaciones que se vieron afectadas por el ransomware en el último año



Porcentaje de ataques que comportaron el cifrado de datos.

Mediana del importe de rescate pagado en Chile en el último año.

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 46 % de los incidentes. Le sigue el compromiso de credenciales, que originó el 22 % de los ataques. Los correos maliciosos se utilizaron en el 20 % de los ataques.
- **Una laguna de seguridad conocida fue la causa raíz operativa más común**, mencionada por el 55 % de los encuestados chilenos. Le siguió la falta de conocimientos especializados, que fue citada por el 46 % de las organizaciones. Según el 44 %, la falta de personal/capacidad para supervisar sus sistemas en el momento del ataque influyó en que su organización sufriera un ataque de ransomware.

Qué ocurre con los datos

- **El 52 % de los ataques comportaron el cifrado de datos.**
- **También se robaron datos en el 17 % de los ataques en que se cifraron datos**, significativamente por debajo de la media global del 28 %.
- **El 97 % de las organizaciones chilenas a las que les cifraron los datos pudieron recuperarlos.**
- **El 56 % de las organizaciones chilenas pagaron el rescate y recuperaron los datos.**
- **El 49 % de las organizaciones chilenas utilizaron copias de seguridad para recuperar los datos cifrados.**

Los rescates: peticiones e importes

- **La mediana de petición de rescate en Chile el año pasado fue de un millón USD,** ligeramente inferior a la media global de 1,32 millones USD.

Mediana de petición de rescate en Chile el año pasado.

- **El 53 % de las peticiones de rescate ascendieron a 1 millón USD o más.**
- **La mediana del importe de rescate pagado en Chile el año pasado fue de 675 000 USD,** muy por debajo de la media global de un millón USD.
- **Por lo general, las organizaciones chilenas pagaron el 80 % de la petición de rescate**, por debajo de la media mundial del 85 %.
  - El 67 % **pagó MENOS de lo que se pedía inicialmente** por el rescate (media global: 53 %).
  - El 19 % **IGUALÓ la petición inicial** (media global: 29 %).
  - El 14 % **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 1,2 millones USD,** por debajo de la media global de 1,53 millones de 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 chilenas se recuperan rápidamente de los ataques de ransomware:** el 65 % se recuperó totalmente en menos de una semana, muy por encima del 53 % de la media global. Solo el 8 % tardó entre uno y seis meses en recuperarse, significativamente por debajo de la media mundial del 18 %.

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

Para el 46 %, ha **aumentado la ansiedad o el estrés** por futuros ataques.

Según el 37 %, **tienen más presión** por parte de los cargos directivos.

El 35 % afirma que la **carga de trabajo del equipo ha aumentado** desde el ataque.

El 33 % tiene **sentimiento de culpa** por no haber detenido el ataque.

El 33 % se han visto afectados por las **bajas de miembros del equipo** por problemas de estrés/salud mental.

Recomendaciones

El ransomware sigue siendo una amenaza importante para las organizaciones chilenas. 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 CL-WP (DD)