SOPHOS

EL ESTADO DEL RANSOMWARE EN MÉXICO 2026

Resultados de una encuesta independiente desvinculada de cualquier proveedor a 84 organizaciones en México que se vieron afectadas por el ransomware en el último año.

MONOGRÁFICOS DE SOPHOS - JULIO DE 2026

Acerca del informe

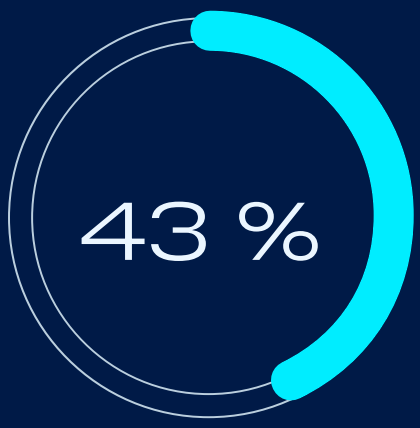
Este séptimo informe anual sobre el estado del ransomware se basa en los resultados de una encuesta independiente encargada por Sophos. El informe global de este año se basa en las experiencias de 2158 responsables de TI y ciberseguridad que trabajan en organizaciones que se vieron afectadas por el ransomware en el último año, entre ellas 84 de México.

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

84

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.

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 mexicanas al ransomware

- **El compromiso de credenciales fue la causa raíz técnica más común: se** utilizó en el 39 % de los ataques, el porcentaje más alto de todos los países encuestados, seguido del correo electrónico malicioso (24 %) y la explotación de vulnerabilidades (18 %). La explotación de vulnerabilidades se redujo al 18 %, frente al 45 % registrado en el informe de 2025.
- **Una laguna de seguridad desconocida (43 %) fue la causa raíz operativa más común,** seguida de una laguna de seguridad conocida (38 %) y de una protección deficiente (35 %).
- **(NOVEDAD) Las aplicaciones y los sistemas expuestos constituyeron, en general, el punto de entrada más habitual (48 %)** en los casos en los que la causa raíz no estaba relacionada ni con el correo electrónico ni con el phishing, seguidos de los dispositivos de los usuarios (26 %) y los firewalls (14 %).
- **(NOVEDAD) El 67 % confirmó que el incidente de ransomware del año pasado coincidió con su ataque más significativo relacionado con la identidad.**

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 50 % registrado por los encuestados mexicanos en 2025.
- **El 58 % de las organizaciones mexicanas utilizaron copias de seguridad para recuperar los datos cifrados,** un descenso notable con respecto al 68 % registrado en 2025.
- **También se produjo el robo de datos en el 33 % de los casos en que se cifraron datos,** lo que supone un descenso considerable con respecto al 52 % registrado en la edición de 2025.
- **El 100 % de las organizaciones mexicanas cuyos datos fueron cifrados pudieron recuperarlos,** en consonancia con la media mundial.
- **El 47 % de las organizaciones mexicanas pagaron el rescate y recuperaron los datos,** lo que supone aumento significativo con respecto al 23 % de 2025.

Peticiones de rescate

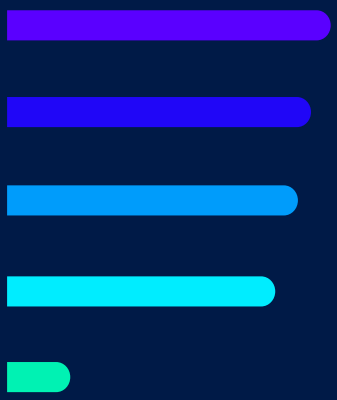
- **La mediana del rescate exigido en México fue de 540 000 USD,** lo que supone una caída del 73 % con respecto a los 2 millones USD que figuraban en el informe de 2025.
- **El 31 % de las peticiones de rescate fueron de un millón USD o más,** lo que supone un descenso considerable con respecto al 70 % registrado en el informe de 2025.

Mediana del importe de rescate en México.

El impacto del ransomware en el negocio

- Sin tener en cuenta los pagos de rescate, **el coste medio de recuperación para las organizaciones mexicanas tras sufrir un ataque de ransomware ascendió a 752 000 millones USD,** muy por debajo de la media de 1,35 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 64 % de las organizaciones mexicanas se recuperó de un ataque de ransomware en un plazo inferior a una semana,** cifra que se mantiene igual que la registrada en el informe de 2025. El 12 % tardó entre uno y seis meses en recuperarse, un ligero aumento con respecto al 10 % del informe de 2025.

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



Según el 47 %, tienen más presión por parte de los cargos directivos. Un aumento respecto al 32 % en 2025.

El 44 % tiene sentimiento de culpa por no haber detenido el ataque. Un aumento respecto al 30 % en 2025.

Para el 42 %, ha aumentado la ansiedad o el estrés por futuros ataques. Un aumento respecto al 32 % en 2025.

El 39 % señala un aumento continuo de la carga de trabajo desde el ataque.

El 8 % afirma que se ha sustituido a los responsables del equipo.

Recomendaciones

Refuerce la seguridad de la identidad como medida de defensa contra el ransomware. Casi dos tercios de las víctimas de ransomware en México 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 más de un tercio de las causas raíz de los ataques de ransomware en México, 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 MX-WP (TA) CRE-6012