SOPHOS

EL ESTADO DEL RANSOMWARE EN ESPAÑA 2026

Resultados de una encuesta independiente desvinculada de cualquier proveedor a 164 organizaciones en España que se vieron afectadas por el ransomware en el último año.

MONOGRÁFICOS DE SOPHOS - JULIO DE 2026

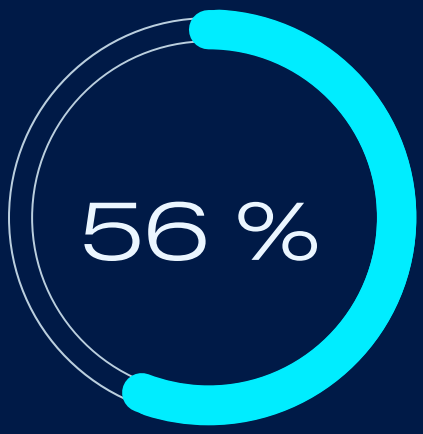
Acerca del informe

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 164 de España.

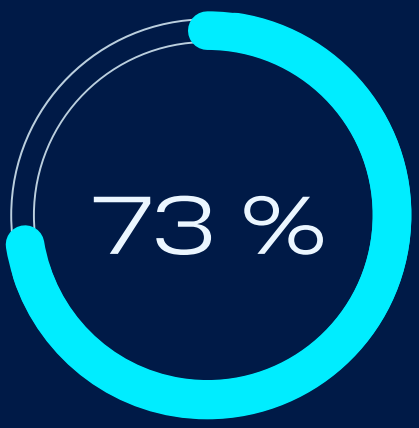
La encuesta se realizó entre enero y marzo de 2026. Todos los encuestados trabajan en organizaciones con entre 100 y 5000 empleados, y se les pidió contestar según sus experiencias en los últimos 12 meses. Todos los puntos de datos financieros son en dólares estadounidenses (USD). Se han eliminado de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

Encuesta a 164

responsables de TI/ciberseguridad en España 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 españolas al ransomware

- **Los correos electrónicos maliciosos fueron la causa raíz técnica más frecuente de los ataques,** ya que se utilizaron en el 29 % de los mismos, seguidos del phishing (24 %) y el compromiso de credenciales (23 %). La explotación de vulnerabilidades disminuyó drásticamente, situándose en el 17 %, frente al 30 % registrado en el informe de 2025.
- **La falta de personal/capacidad (43 %) fue la causa raíz operativa más común,** seguida de una laguna de seguridad desconocida (38 %) y de la falta de conocimientos especializados (38 %).
- **(NOVEDAD) Las aplicaciones y los sistemas expuestos constituyeron, en general, el punto de entrada más habitual (46 %)** 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 (25 %) y los firewalls (17 %).
- **(NOVEDAD) El 73 % 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 56 % de los ataques comportaron el cifrado de datos.** Este dato se ajusta a la media mundial del 56 % y supone un aumento con respecto al 47 % registrado por los encuestados en España en el informe de 2025.
- **También se produjo el robo de datos en el 33 % de los casos en que se cifraron datos,** lo que supone un descenso con respecto al 36 % registrado en el informe de 2025.
- **El 98 % de las organizaciones españolas cuyos datos fueron cifrados pudieron recuperarlos,** en consonancia con la media mundial.
- **El 33 % de las organizaciones españolas pagaron el rescate y recuperaron los datos,** un ligero descenso con respecto al 36 % registrado el año anterior.
- **El 70 % de las organizaciones españolas utilizaron copias de seguridad para recuperar los datos cifrados,** una cifra que se mantiene sin cambios respecto al 70 % registrado en 2025.

Peticiones de rescate

- **La mediana del rescate exigido en España fue de 1,85 millones USD,** lo que supone un aumento del 103 % con respecto a los 911 600 USD que figuraban en el informe de 2025.
- **El 57 % de las peticiones de rescate fueron de un millón USD o más,** lo que supone un aumento con respecto al 50 % registrado en 2025.

Mediana del importe de rescate en España.

El impacto del ransomware en el negocio

- Sin tener en cuenta los pagos de rescate, **el coste medio de recuperación para las organizaciones españolas tras sufrir un ataque de ransomware ascendió a 2,28 millones USD,** lo que supone un aumento significativo con respecto a la media de 1,15 millones USD registrada en 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 50 % de las organizaciones españolas se recuperó de un ataque de ransomware en un plazo inferior a una semana,** lo que supone un ligero aumento con respecto al 49 % registrado en el informe de 2025. El 20 % tardó entre uno y seis meses en recuperarse, un ligero descenso con respecto al 24 % registrado en 2025.

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

El 39 % afirma haber obtenido un mayor reconocimiento por parte de los cargos directivos.

Para el 35 %, ha aumentado la ansiedad o el estrés por futuros ataques.

Según el 35 %, tienen más presión por parte de los cargos directivos.

El 35 % experimentó cambios en la estructura del equipo o la organización. Un aumento respecto al 25 % en 2025.

El 21 % afirma que se ha sustituido a los responsables del equipo.

Recomendaciones

Refuerce la seguridad de la identidad como medida de defensa contra el ransomware. Más de tres cuartas partes de las víctimas de ransomware en España 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 casi la mitad de las causas raíz de los ataques de ransomware en España, 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.

2026-08-04 ES-WP (TA) CRE-6080