SOPHOS

EL ESTADO DEL RANSOMWARE EN ESPAÑA 2025

Resultados de una encuesta independiente desvinculada de cualquier proveedor a 237 organizaciones en España 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 237 de España.

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

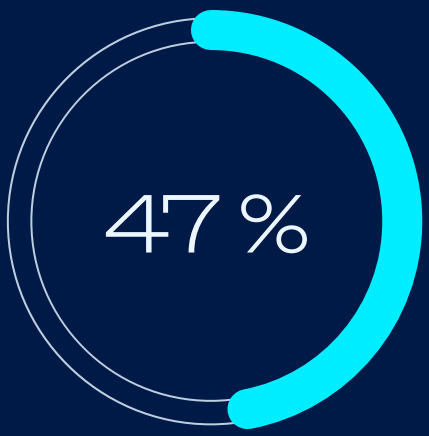
Todos los encuestados trabajan en organizaciones con entre 100 y 5000 empleados, y se les pidió contestar según sus experiencias en los últimos 12 meses.

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

237

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.

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

Coste medio de recuperación de un ataque de ransomware.

Por qué sucumben las organizaciones españolas al ransomware

- **La explotación de vulnerabilidades fue la causa raíz técnica más común de los ataques**, utilizada en el 30 % de los incidentes. Le sigue el compromiso de credenciales, que originó el 21 % de los ataques. Los correos maliciosos se utilizaron en el 17 % de los ataques.
- **Una laguna de seguridad conocida fue la causa raíz operativa más común**, mencionada por el 42 % de los encuestados españoles. Le siguió la falta de personal/capacidad, que fue citada por el 41 % de las organizaciones. Según el 39 %, la falta de conocimientos especializados y una laguna de seguridad desconocida influyeron en que su organización sufriera un ataque de ransomware.

Qué ocurre con los datos

- **El 47 % de los ataques comportaron el cifrado de datos.** Esta cifra es inferior a la media mundial del 50 %, pero supone un descenso significativo con respecto al 89 % registrado por los encuestados españoles en 2024.
- **También se produjo el robo de datos en el 36 % de los casos en que se cifraron datos,** justo por encima del 34 % registrado el año pasado.
- **Todas las organizaciones españolas a las que les cifraron los datos pudieron recuperarlos.**
- **El 36 % de las organizaciones españolas pagaron el rescate y recuperaron los datos,** un descenso considerable frente al 56 % registrado el año anterior.
- **El 70 % de las organizaciones españolas utilizaron copias de seguridad para recuperar los datos cifrados,** lo que supone una disminución con respecto al 73 % del año anterior.

Los rescates: peticiones e importes

- **El año pasado, la mediana de petición de rescate en España fue de 911 600 USD**, menos de una cuarta parte de los 4,24 millones USD registrados en nuestra encuesta de 2024.

Mediana del importe de rescate en España el año pasado.

- **El 50 % de las peticiones de rescate fueron de un millón USD o más**, frente al 73 % de 2024.
- **La mediana del importe de rescate pagado en España durante el último año fue de 322 500 USD**, considerablemente inferior a los 4,4 millones USD registrados en el año anterior.
- **Por lo general, las organizaciones españolas pagaron el 80 % de la petición de rescate**, por debajo de la media mundial del 85 %.
  - El 72 % **pagó MENOS de lo que se pedía inicialmente** por el rescate (media global: 53 %).
  - El 28 % **IGUALÓ la petición inicial** (media global: 29 %).
  - El 0 % **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 españolas para recuperarse de un ataque de ransomware el año pasado fue de 1,15 millones USD,** un descenso notable respecto a los 3,43 millones USD notificados por los encuestados españoles en 2024. 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 españolas se recuperan cada vez más rápido de un ataque de ransomware:** el 49 % se recuperaron totalmente en menos de una semana, lo que supone un aumento respecto al 27 % del año anterior. El 24 % tardó entre uno y seis meses en recuperarse, un descenso considerable respecto al 45 % del año pasado.

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

Según el 36 %, han visto un **aumento continuo de la carga de trabajo.**

Para el 33 %, ha **aumentado la ansiedad o el estrés por futuros ataques.**

Según el 28 %, **tienen más presión** por parte de los cargos directivos.

El 27 % tiene **sentimiento de culpa** por no haber detenido el ataque.

Según el 25 %, ha habido **bajas del personal por estrés o problemas de salud mental**.

Recomendaciones

El ransomware sigue siendo una amenaza importante para las organizaciones españolas. 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.

2025-07-11 ES-WP (DD)