Agosto de 2025

Informe de mercado

# Informe de Barracuda sobre Ransomware 2025

Análisis de la experiencia y el impacto del ransomware en organizaciones de todo el mundo

Barracuda®
Your business, secured.

# Contenido

# Introducción

El ransomware es una amenaza generalizada y en constante evolución, impulsada por kits de ransomware as a service que permiten a cada vez más ciberdelincuentes lanzar ataques. Los incidentes de ransomware pueden dañar la reputación de las marcas y perturbar las operaciones diarias, lo que provoca interrupciones, pérdida de datos, pérdida de confianza de los clientes y mucho más. Todas las organizaciones son un objetivo potencial.

Este informe analiza la experiencia y el impacto de los ataques de ransomware consumados en organizaciones de todo el mundo durante los últimos 12 meses. Se basa en los resultados de una encuesta internacional realizada por Barracuda y Vanson Bourne a 2.000 responsables de la toma de decisiones en materia de TI y seguridad.

Los resultados pueden agruparse en tres temas generales, a saber:

- **Las víctimas del ransomware suelen tener una seguridad fragmentada**, con demasiadas herramientas desconectadas y una cobertura insuficiente en áreas clave de seguridad.
- **Los ataques de ransomware son multidimensionales.** Ya no se limitan al cifrado de datos, sino que ahora implican el robo y la exposición de datos, la instalación de cargas maliciosas adicionales y mucho más.
- **El impacto de un ataque de ransomware consumado se está ampliando,** incluyendo la pérdida de nuevas oportunidades de negocio y tácticas de extorsión para el pago, que se extienden a los empleados, socios, clientes y autoridades.

## Metodología

Barracuda encargó a la empresa independiente de estudios de mercado Vanson Bourne la realización de una encuesta global a 2.000 responsables de la toma de decisiones en materia de seguridad que ocupan puestos de TI y negocio en organizaciones de entre 50 y 2.000 empleados de una amplia gama de sectores en Estados Unidos, Reino Unido, Francia, DACH (Alemania, Austria, Suiza), Benelux (Bélgica, Países Bajos y Luxemburgo), los países nórdicos (Dinamarca, Finlandia, Noruega y Suecia), Australia, India y Japón. El trabajo de campo se llevó a cabo en abril y mayo de 2025.

# Introducción

Esperamos que este informe ayude a organizaciones de todos los tamaños y sectores a comprender la amenaza y el impacto del ransomware en 2025, así como a identificar y abordar las áreas que posiblemente estén en riesgo.

# Principales conclusiones

57 %

de las organizaciones experimentaron un ataque de ransomware exitoso en los últimos 12 meses

71 %

de las organizaciones que habían sufrido una filtración de correo electrónico también se vieron afectadas por el ransomware

32 %

pagaron un rescate para recuperar sus datos, y el 41 % de ellas no recuperó todos sus datos

65 %

de las víctimas de ransomware pudieron restaurar los datos a partir de copias de seguridad

24 %

de las víctimas de ransomware tuvieron datos cifrados, mientras que al 27 % les robaron datos y el 29 % afirmó que los atacantes instalaron cargas útiles adicionales

25 %

de las víctimas de ransomware perdieron clientes existentes, y el mismo porcentaje perdió nuevas oportunidades de negocio

# El ransomware afecta a más de la mitad de las organizaciones

**En general, el 57 % de las organizaciones encuestadas había sufrido un ataque de ransomware consumado en los últimos 12 meses.**

Una de cada tres víctimas (31 %) se vio afectada dos o más veces.

La prevalencia de múltiples ataques consumados sugiere que las brechas de seguridad no se investigan ni abordan completamente después de cada incidente. A lo largo de este informe, analizamos la diferencia entre las organizaciones afectadas una vez y las afectadas varias veces para ver qué se puede aprender de los datos y cómo pueden las organizaciones utilizarlos para mejorar su postura de seguridad.

Los sectores más afectados en nuestra encuesta fueron el sanitario (con un 67 % de las organizaciones afectadas), la administración local (65 %) y el comercio minorista (61 %). Según los datos, la industria manufacturera fue la menos afectada, con algo menos de la mitad (46 %) de los encuestados que informaron de un ataque consumado.

El tamaño no parece ser un factor determinante en lo que respecta al ransomware, ya que los resultados son similares en todas las empresas encuestadas, independientemente de su tamaño, desde 50 hasta 2.000 empleados.

**El 71 % de las organizaciones que habían sufrido una brecha de seguridad en el correo electrónico también se vieron afectadas por el ransomware, lo que pone de relieve la relación entre ambos tipos de ataques.**

## Las víctimas del ransomware tienen un perfil diferente en cuanto a herramientas de seguridad y prioridades

### La proliferación de la seguridad y el riesgo del ransomware

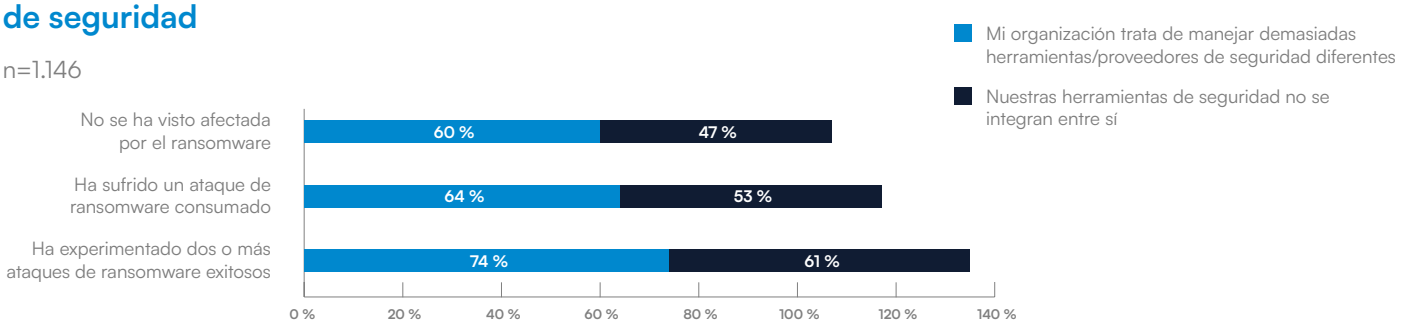
La encuesta muestra que el exceso de herramientas de seguridad, conocido como proliferación de la seguridad, acompañado de una falta de integración, puede aumentar el riesgo y crear brechas en la protección, ya que dificulta a las organizaciones la detección y mitigación de amenazas activas, incluido el ransomware.

Los datos muestran que la proporción de organizaciones afectadas por la proliferación de la seguridad o la falta de integración aumenta en función de su experiencia con el ransomware.

FIGURA 1

## Incidentes de ransomware y proliferación de herramientas de seguridad

n=1.146



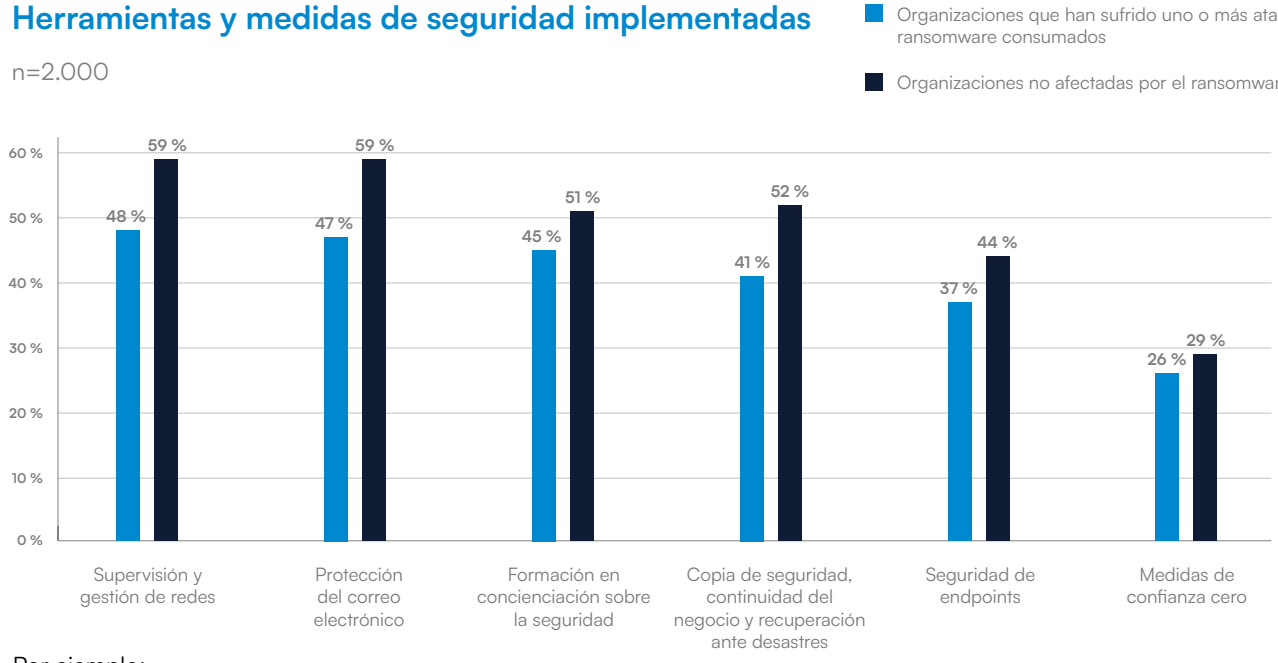

## Los diferentes tipos de herramientas y medidas de seguridad

Según los encuestados, las medidas de seguridad más implantadas son la protección del correo electrónico (implementada por el 52 %), la seguridad de la red (52 %) y la formación en concienciación sobre seguridad (48 %). Las organizaciones que han sufrido un incidente de ransomware consumado son menos propensas a haber implementado alguna de estas medidas.

FIGURA 2

## Herramientas y medidas de seguridad implementadas

n=2.000




Por ejemplo:

- El 47 % de las víctimas de ransomware había implementado una solución de seguridad para el correo electrónico, en comparación con el 59 % de las que no lo habían sufrido
- El 48 % de las víctimas de ransomware contaba con gestión y supervisión de la red, en comparación con el 59 % de las que no lo habían sufrido
- El 45 % de las víctimas de ransomware contaba con formación en concienciación sobre seguridad, en comparación con el 51 % de las que no lo habían sufrido
- El 37 % había implementado seguridad para endpoints, en comparación con el 44 % de las que no lo habían sufrido

**Estos resultados sugieren que las víctimas de ransomware podrían estar invirtiendo poco en áreas de seguridad que las ayudarían a reducir su exposición al riesgo.**

Por ejemplo, la seguridad del correo electrónico, la red y los endpoints, junto con la formación en concienciación sobre seguridad, proporcionan una defensa sólida contra los ataques de phishing y de ingeniería social a través del correo electrónico, que están diseñados para robar credenciales y permitir a los atacantes irrumpir en las redes, comprometer los dispositivos y moverse lateralmente, todas ellas técnicas características de un ataque de ransomware.

## Las bandas de ransomware tienen una probabilidad de una entre tres de cobrar el rescate

**El 32 % de las víctimas de ransomware pagaron un rescate para recuperar o restaurar los datos.**

Los resultados muestran una correlación entre la propensión de una organización a pagar un rescate y el número de veces que se ve afectada por el ransomware.

Las organizaciones que solo sufrieron un ataque de ransomware consumado eran ligeramente menos propensas a pagar el rescate, con un 29 %, mientras que, de las que se vieron afectadas dos o más veces, el 37 % pagó el rescate para recuperar sus datos.

Estas cifras han cambiado poco desde la última encuesta hace dos años. En 2023, los resultados mostraban que el 31 % de los afectados una vez y el 38 % de los afectados dos o más veces pagaron un rescate para recuperar los datos.

Una posible explicación de la relación entre los ataques múltiples y los pagos de rescates es que, una vez que se demuestra que una organización está dispuesta a pagar, otros atacantes se centran en la misma víctima, o el mismo atacante puede volver más de una vez.

La buena noticia es que la mayoría (65 %) de los afectados por el ransomware pudieron restaurar sus datos utilizando copias de seguridad.

Como claro recordatorio de que pagar el rescate no sale a cuenta: el 41 % de los que pagaron (el 13 % del total) no recuperaron todos sus datos, ni siquiera en parte.

## El cifrado de datos es ahora solo una parte de un ataque de ransomware

Aparte de la carga económica que supone pagar un rescate, la investigación muestra que el impacto comercial, operativo e incluso emocional de un ataque de ransomware consumado es considerable.

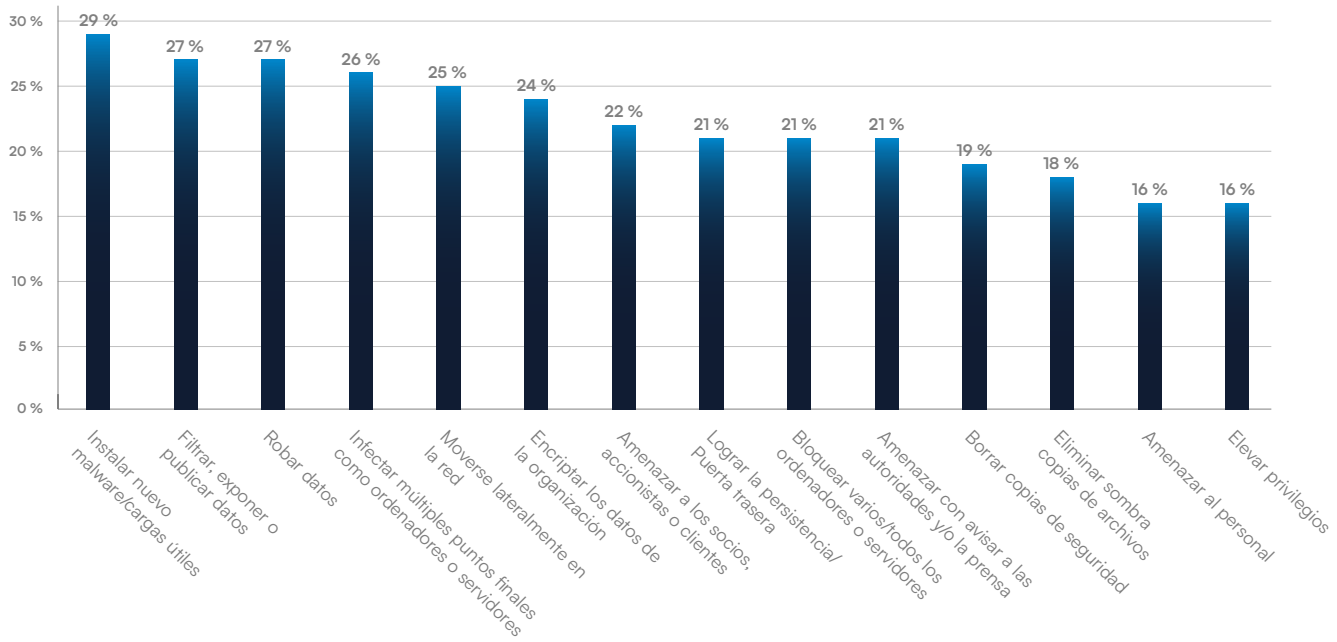
En la mayoría de los incidentes de ransomware, el cifrado de los datos y el bloqueo de los sistemas y ordenadores suele ser el objetivo final. Esta es la parte más visible del ataque y, por lo tanto, la más susceptible de revelar la presencia de intrusos al equipo de seguridad y dar lugar a la contención y eliminación de la amenaza.

Los resultados de la investigación ponen de relieve la amplitud de las actividades que se llevan a cabo de forma sigilosa antes de ejecutar el ransomware, ya sea para permitir el ataque o para allanar el camino a otras actividades.

FIGURA 3

## Actividades realizadas por las bandas de ransomware durante los incidentes más significativos

n=1.146




### Alrededor de una cuarta parte de los incidentes de ransomware experimentados por los encuestados implicaron el cifrado de datos (24 %), el bloqueo de endpoints (21 %) y el robo de datos (27 %).

Los ataques también se caracterizan por el movimiento lateral a través de la red (25 %), la infección de múltiples terminales, como ordenadores o servidores (26 %), la instalación de cargas maliciosas adicionales (29 %), la elevación de privilegios (16 %) y la incorporación de puertas traseras y otros mecanismos de persistencia (21 %).

Además, para dificultar a las víctimas la restauración de sus datos sin pagar, aproximadamente uno de cada cinco atacantes accedió y borró las copias de seguridad y eliminó las copias ocultas de los archivos (el 19 % de las víctimas sufrieron ambos procesos).

Los resultados también muestran que, una vez que se ha ejecutado el ransomware y se ha enviado la exigencia del rescate, los atacantes comienzan a ejercer presión sobre la víctima mediante tácticas psicológicas. Entre ellas se incluyen amenazas a socios, accionistas o clientes (experimentadas por el 22 %), amenazas de alertar a la prensa o a las autoridades (21 %) e incluso amenazas al personal (16 %).

En el 27 % de los incidentes de ransomware que tuvieron éxito, los atacantes procedieron a filtrar, exponer o publicar los datos robados.

# Las víctimas de ransomware pierden clientes y nuevas oportunidades de negocio

Una vez el ataque se ha consumado, las víctimas se enfrentan a repercusiones operativas y comerciales.

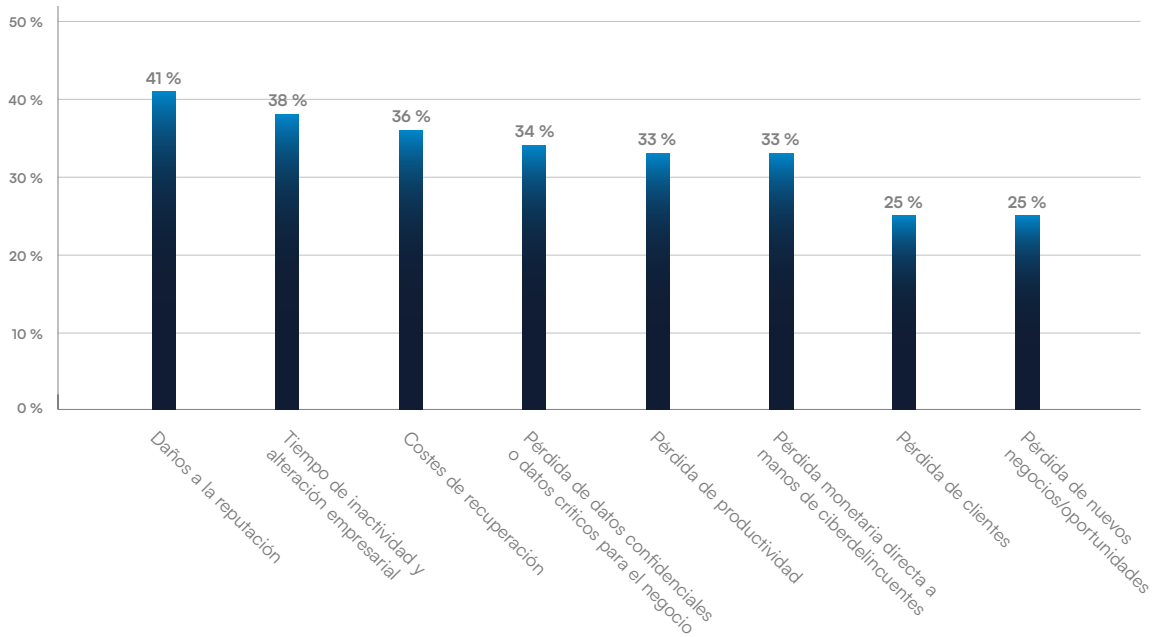
El principal impacto citado por las víctimas del ransomware fue el daño a su marca y reputación (que afectó al 41 %). Le siguen el tiempo de inactividad (38 %) y los costes de recuperación (36 %). Un tercio (34 %) admitió haber perdido datos confidenciales.

**Una de cada cuatro víctimas del ransomware sufrió el impacto comercial a largo plazo de perder clientes existentes y nuevas oportunidades de negocio (ambos en un 25 %).**

FIGURA 4

## El impacto del ataque de ransomware más significativo de los últimos 12 meses

n=1.146



# Conclusión

Para ser resistentes al ransomware, las organizaciones necesitan una seguridad integrada y multicapa que proteja su superficie de ataque en constante expansión frente a las ciberamenazas.

Los siguientes pasos prácticos pueden ayudar:

- **Asegúrese de que los datos se copian de forma periódica y segura** y se mantienen fuera de línea. Haga pruebas para asegurarse de que puede restaurar los datos de forma eficaz.
- **Implemente la autenticación multifactor y aplique el principio del privilegio mínimo** para limitar el acceso a los activos y aplicaciones de la empresa. Así se evita que los atacantes se dirijan a datos y sistemas de alto valor, incluso con credenciales robadas.
- **Mantenga el software actualizado** con los últimos parches de seguridad para cerrar las brechas de seguridad.
- **Imparta formación periódica sobre ciberseguridad** a los empleados, centrándose en las últimas tácticas de phishing y ransomware.
- **Segmente la red,** aislando los sistemas críticos para evitar el movimiento lateral de los atacantes.
- **Compruebe todas las configuraciones,** incluidas las de la nube. Las configuraciones incorrectas son uno de los principales factores que contribuyen a las brechas de seguridad.
- **Instale una robusta solución de seguridad para el correo electrónico.** El correo electrónico sigue siendo uno de los principales puntos de entrada del ransomware, y una protección avanzada basada en IA puede detectar cargas maliciosas y reconocer tácticas avanzadas de ingeniería social diseñadas para eludir la seguridad.
- **Proteja las aplicaciones web,** como los servicios de intercambio de archivos, los formularios web y los sitios de comercio electrónico. Las aplicaciones suelen ser objeto de ataques a través de la interfaz de usuario o una API.
- **Disponga de un plan de respuesta ante incidentes y pruébelo periódicamente.**
- **Considere la posibilidad de colaborar con expertos externos**, incluidos proveedores de servicios gestionados y proveedores de seguridad, para obtener soporte adicional. Estos socios pueden ayudarle a implementar plataformas y soluciones de seguridad integradas avanzadas para detectar, bloquear y responder a las amenazas activas 24 horas al día, 7 días a la semana, conteniendo y neutralizando los incidentes antes de que puedan causar daños graves.

# Sobre Barracuda

Barracuda es una empresa líder mundial en ciberseguridad que ofrece protección completa contra amenazas complejas para empresas de todos los tamaños. Nuestra plataforma impulsada por IA asegura el correo electrónico, los datos, las aplicaciones y las redes con soluciones innovadoras, XDR gestionado y un panel de control centralizado para maximizar la protección y fortalecer la ciberresiliencia. Con la confianza de cientos de miles de profesionales de TI y proveedores de servicios gestionados de todo el mundo, Barracuda ofrece defensas potentes que son fáciles de comprar, implementar y usar.



# Sobre Vanson Bourne

Vanson Bourne es un especialista independiente en investigación de mercados para el sector tecnológico. Su reputación en lo referente a análisis sólidos y creíbles basados en la investigación reside en rigurosos principios de investigación y en su capacidad para recabar las opiniones de los principales responsables de la toma de decisiones en todas las funciones técnicas y empresariales, en todos los sectores empresariales y en los principales mercados. Para obtener más información, visite vansonbourne.com.