SOPHOS
Cybersecurity evolved.

# El estado del ransomware 2021

La encuesta anual sobre el ransomware de Sophos aporta nueva información detallada sobre las experiencias de empresas de tamaño mediano de todo el planeta. Explica la prevalencia de los ataques, además del impacto que tienen estos en las víctimas, incluidas las tendencias interanuales. Este año, por primera vez, la encuesta también revela los pagos reales de rescates abonados por las víctimas, además del porcentaje de datos que estas lograron recuperar después de pagar.

*Monográficos de Sophos. Abril 2021*

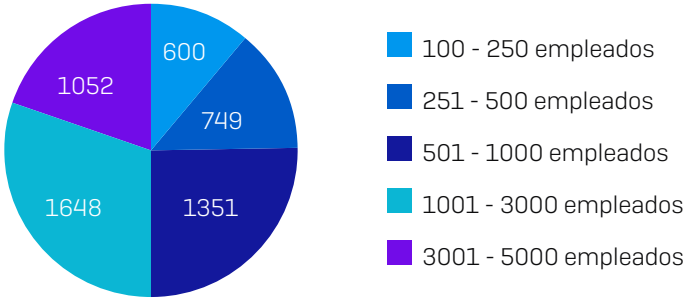
# Acerca de la encuesta

Sophos encargó a la consultora independiente Vanson Bourne la realización de una encuesta a 5400 directores de TI de 30 países. La encuesta se llevó a cabo en enero y febrero de 2021.

| PAÍS | N.º DE ENCUESTADOS | PAÍS | N.º DE ENCUESTADOS | PAÍS | N.º DE ENCUESTADOS |
|---|---|---|---|---|---|
| Australia | 250 | India | 300 | Arabia Saudita | 100 |
| Austria | 100 | Israel | 100 | Singapur | 150 |
| Bélgica | 100 | Italia | 200 | Sudáfrica | 200 |
| Brasil | 200 | Japón | 300 | España | 150 |
| Canadá | 200 | Malasia | 150 | Suecia | 100 |
| Chile | 200 | México | 200 | Suiza | 100 |
| Colombia | 200 | Países Bajos | 150 | Turquía | 100 |
| República Checa | 100 | Nigeria | 100 | EAU | 100 |
| Francia | 200 | Filipinas | 150 | Reino Unido | 300 |
| Alemania | 300 | Polonia | 100 | Estados Unidos | 500 |

Igual que en años anteriores, el 50 % de los encuestados de cada país procedían de empresas con entre 100 y 1000 empleados y el otro 50 %, de empresas con entre 1001 y 5000 empleados. Los encuestados también pertenecían a una amplia gama de sectores.

### ¿Cuántos empleados tiene su empresa en todo mundo?




### ¿A qué sector pertenece su empresa?

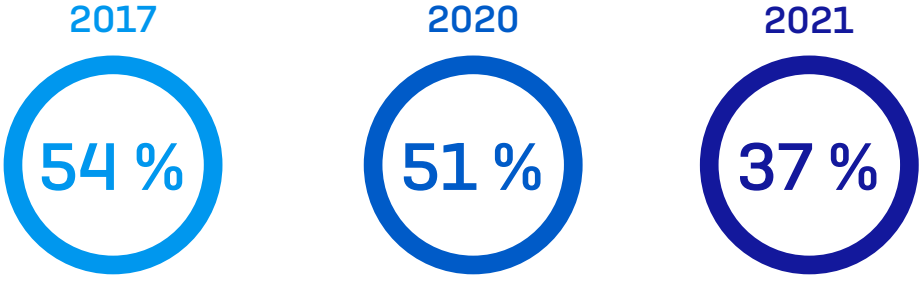
# Principales conclusiones

- El **37 %** de las empresas de los encuestados se **vieron afectadas por el ransomware en el último año**.
- El **54 %** de las que se vieron afectadas por el ransomware en el último año afirmaron que los **ciberdelincuentes consiguieron cifrar sus datos** en el ataque más importante.
- El **96 %** de aquellas empresas cuyos datos fueron cifrados **recuperaron sus datos** en el ataque de ransomware más importante.
- El **rescate medio pagado** por las empresas de tamaño mediano fue de **170 404 USD**.
- Sin embargo, de media, solo el **65 % de los datos cifrados fueron restaurados** después de pagar el rescate.
- La **factura media de rectificar un ataque de ransomware**, teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, etc. fue de **1,85 millones USD**.
- **Los ataques de tipo extorsión** en que los datos no se cifraron pero aun así se exigió un rescate a la víctima **se han más que duplicado** desde el año pasado, con una incremento del 3 % al 7 %.
- Contar con **personal de TI formado capaz de detener los ataques** es el principal motivo por el que algunas empresas confían en que no se verán afectadas por el ransomware en el futuro.

# La prevalencia del ransomware

## El ransomware sigue siendo una importante amenaza

El 37 % de las empresas (más de un tercio de las 5400 encuestadas) se vieron afectadas por el ransomware el año pasado, en el sentido de que **múltiples ordenadores recibieron un ataque de ransomware, pero no se cifraron datos necesariamente**. Aunque se trata de un número elevado, la buena noticia es que supone una notable reducción con respecto al año anterior, en que el 51 % afirmó haber sufrido ataques.

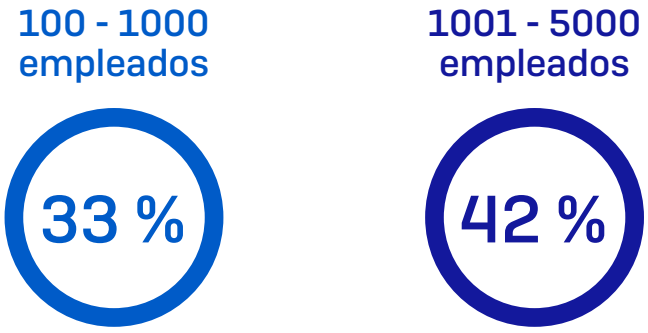



*En el último año, ¿se ha visto afectada por el ransomware su empresa? Sí [2021=5400; 2020=5000; 2017=2700], omitiendo algunas opciones de respuesta, divididas por año*

Los cambios en los comportamientos de los atacantes observados por los equipos de SophosLabs y Sophos Managed Threat Response indican que la reducción en el número de ataques podría deberse en parte a la evolución de los enfoques de ataque. Por ejemplo, muchos delincuentes han pasado de los ataques automatizados, genéricos y a gran escala a ataques más dirigidos que incluyen hacking manual realizado por humanos. Si bien el número total de ataques es inferior, según nuestra experiencia, el potencial de daños de estos ataques dirigidos es muy superior.

## Las empresas más grandes tienen más posibilidades de sufrir ataques

Si miramos el número de incidentes de ransomware por tamaño de empresa, observamos que las más grandes informaron de una mayor prevalencia de ataques: el 42 % de empresas del grupo de 1001-5000 empleados admitieron haberse visto afectadas frente al 33 % en el caso de las empresas más pequeñas.

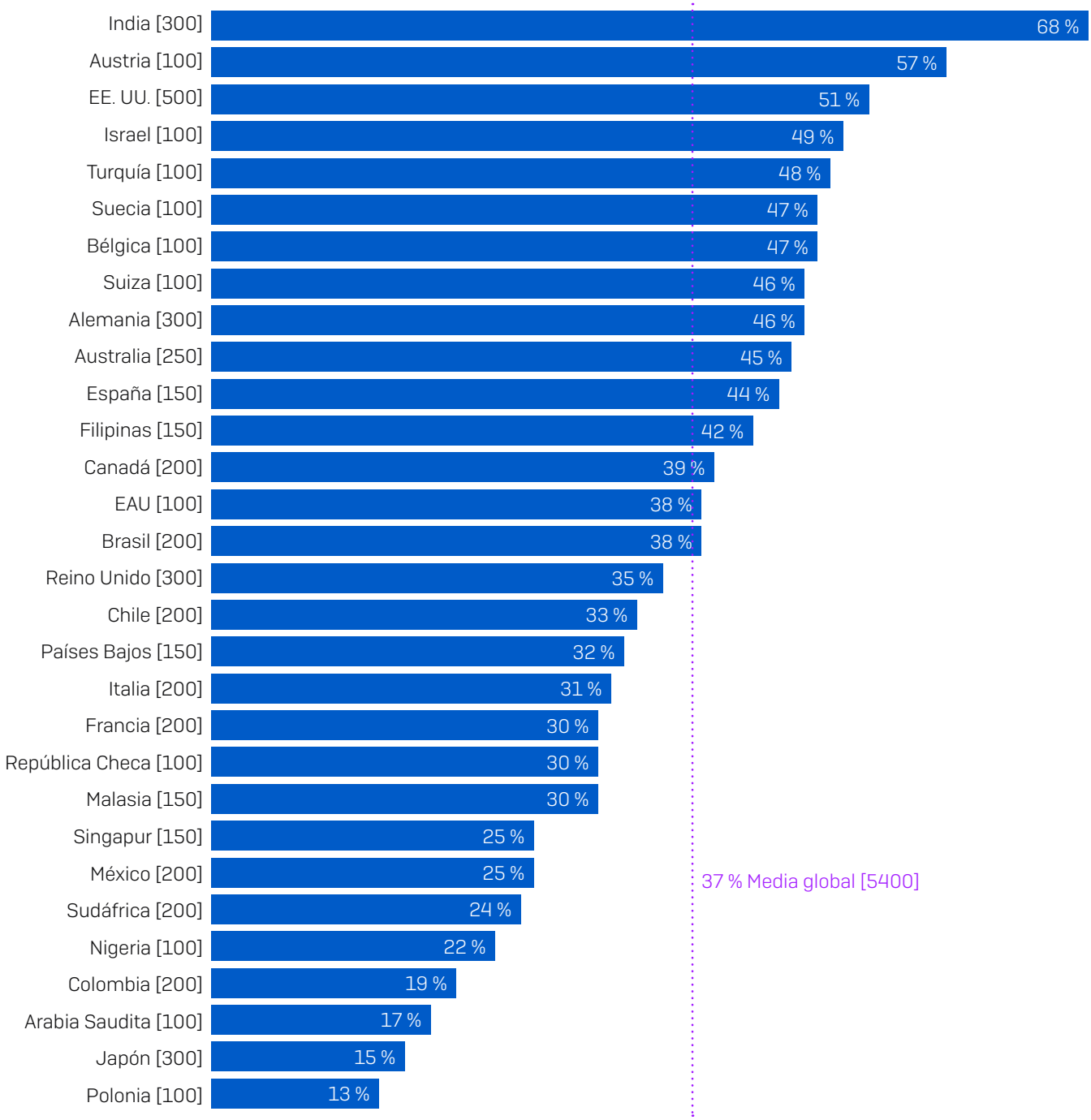



*En el último año, ¿se ha visto afectada por el ransomware su empresa? Sí [5400], omitiendo algunas opciones de respuesta, divididas por tipo de empresa*

Este año la diferencia entre las empresas más pequeñas y las más grandes también se ha incrementado de 7 puntos porcentuales en 2020 a 9 puntos porcentuales. Este mayor interés de los atacantes por las empresas de mayor tamaño quizás no sea ninguna sorpresa: las empresas más grandes tienen más probabilidades de tener más dinero y, por tanto, de ser un objetivo más lucrativo. Dicho esto, una de cada tres empresas pequeñas se vio afectada por el ransomware en el último año, lo que confirma sin lugar a dudas que siguen estando bajo el radar de los atacantes. Aquí no hay ganadores.

## Los niveles de ataque varían en todo el mundo

El análisis de los datos en función del país en que se encontraba el encuestado también revela algunos resultados interesantes.




*En el último año, ¿se ha visto afectada por el ransomware su empresa? Sí [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por país*

La **India** tiene el dudoso honor de encabezar la lista, ya que el 68 % de los encuestados afirmaron haber sido víctimas del ransomware en el último año. Aunque los responsables del ransomware que salen en las noticias suelen encontrarse en China, Corea del Norte, Rusia y otros países del antiguo bloque del Este, SophosLabs observa altos niveles de ransomware nacional en la India, es decir, adversarios indios que atacan a empresas indias.

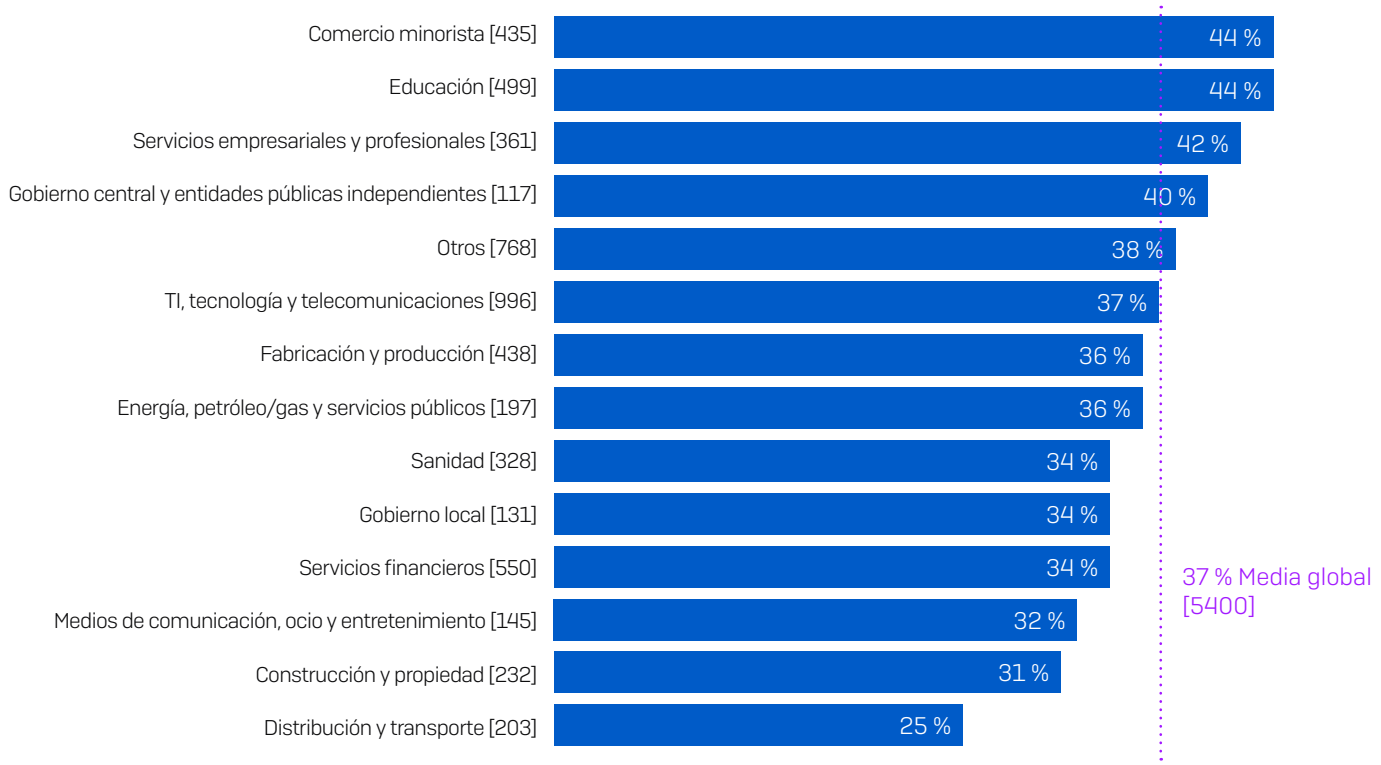
Los **EE. UU.** es un objetivo muy popular entre los ciberdelincuentes debido al potencial percibido para exigir elevados rescates, y un poco más de la mitad (51 %) de los encuestados de EE. UU. afirmaron que fueron atacados el año pasado.

**Polonia, Colombia, Nigeria, Sudáfrica** y **México** registran los niveles de ataque más bajos, lo que probablemente se debe a que tienen un PIB inferior y, por tanto, ofrecen un menor potencial de pago por rescate a los atacantes.

**Japón** destaca por ser una economía desarrollada con unos niveles de ransomware muy bajos: solo el 15 % de los encuestados afirmaron haber sufrido algún ataque de ransomware el año pasado. Japón es un país que suele registrar unos niveles de ransomware muy bajos en nuestras encuestas anuales. Esto puede deberse a que las empresas japonesas han realizado cuantiosas inversiones en defensas antiransomware, o a que el carácter singular de la lengua japonesa convierte al país en un objetivo más complejo para los adversarios.

## El comercio minorista y la educación sufren la mayoría de ataques de ransomware

Si miramos el nivel de ataques por sector, observamos una considerable variación en la predisposición a sufrir un ataque de ransomware en las distintas industrias.




*En el último año, ¿se ha visto afectada por el ransomware su empresa? Sí [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por sector*

*El* **comercio minorista** y la **educación** sufrieron la mayor cantidad de ataques, ya que el 44 % de los encuestados de estos sectores afirmaron haberse visto afectados.

La **sanidad**, que a menudo aparece en las noticias por los ataques de ransomware que recibe, en realidad registró unos niveles de ataque ligeramente inferiores a la media: el 34 % de los encuestados afirmaron que su organización había sido atacada. Esta excesiva exposición del sector en las noticias se debe probablemente a obligaciones normativas que requieren a las entidades sanitarias revelar los ataques, mientras que muchas empresas comerciales pueden mantenerlas en privado.

# El impacto del ransomware

## El cifrado va en descenso. La extorsión va en aumento.

Preguntamos a las empresas víctimas del ransomware si los delincuentes lograron cifrar sus datos. El 54 % dijo que sí. El 39 % pudo detener el ataque antes de que se pudieran cifrar sus datos, mientras que el 7 % afirmó que sus datos no fueron cifrados, pero que se les exigió un rescate de todas maneras.

Si comparamos estas cifras con los resultados de nuestra encuesta de 2020, nos percatamos de un hecho realmente interesante.

| 2020 | 2021 | |
|---|---|---|
| 73 % | 54 % | Ciberdelincuentes que lograron cifrar datos |
| 24 % | 39 % | Ataque detenido antes de que se pudieran cifrar datos |
| 3 % | 7 % | Datos no cifrados pero se pidió un rescate igualmente |

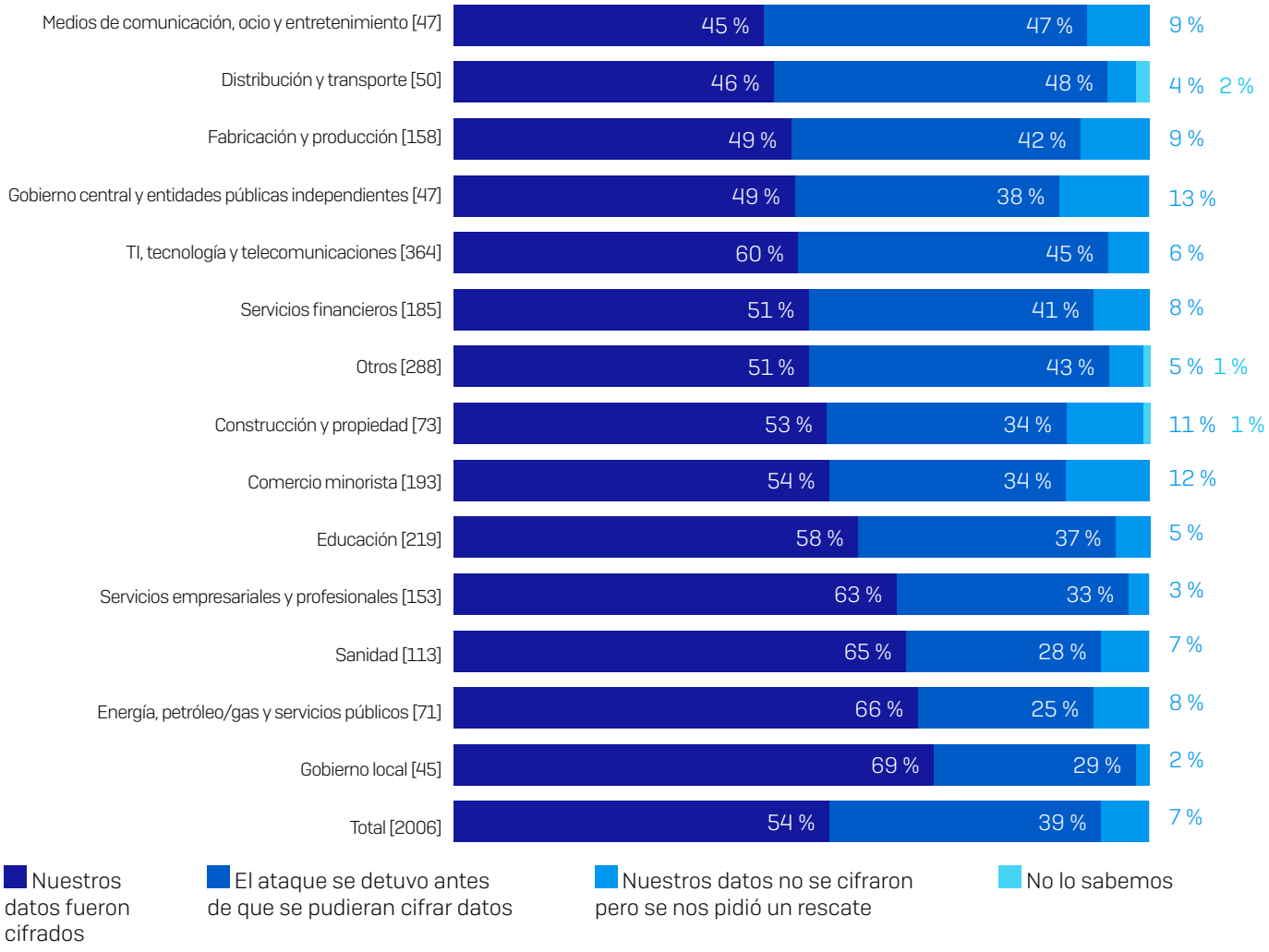
*¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware más importante? [2021=2006; 2020=2538] empresas que se habían visto afectadas por el ransomware en el último año*

En primer lugar, en el último año, se ha producido una importante reducción del porcentaje de ataques en que los delincuentes han logrado cifrar los datos, del 73 % al 54 %, y ahora muchas más empresas consiguen detener el ataque antes de que se cifren los datos. Esto indica que la adopción de tecnología antiransomware está dando resultados.

Sin embargo, también vemos que el porcentaje de ataques en que los datos no se cifraron pero se exigió un rescate a la víctima igualmente se ha más que duplicado. Algunos atacantes se están pasando a los ataques de tipo extorsión, en que en lugar de cifrar archivos, los roban y luego amenazan con publicarlos a menos que se pague el rescate exigido.  Esto requiere menos esfuerzo por su parte, ya que no necesitan cifrar ni descifrar nada. A menudo, los adversarios se aprovechan de las sanciones oficiales por filtraciones de datos en sus exigencias a fin de presionar aún más a las víctimas para que paguen.

## La capacidad de detener el cifrado varía enormemente según el sector

A la hora de detener el cifrado de archivos, algunos sectores son mucho más eficientes que otros.




*¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware más importante? [números base en el gráfico] empresas que se habían visto afectadas por el ransomware en el último año*

El sector de **distribución y transporte** es el que tiene más capacidad para evitar que los atacantes cifren archivos (48 %), seguido de cerca por el de **medios de comunicación, ocio y entretenimiento** (47 %).

En cambio, el **gobierno local** es el sector en que las organizaciones tienen más probabilidades de que se cifren sus datos en un ataque de ransomware (69 %). Esto probablemente se debe al doble impacto de:

- Defensas más débiles: en general, las entidades de los gobiernos locales cuentan con presupuestos de TI más bajos y una plantilla de TI desbordada/limitada.
- Estar más en la mira del atacante: debido a su tamaño y su acceso a fondos públicos, las organizaciones gubernamentales suelen considerarse objetivos lucrativos y, por tanto, son el blanco de ataques más sofisticados. Además, tal como veremos más adelante, el gobierno local también es el segundo sector más propenso a pagar el rescate.

El **gobierno central y entidades públicas independientes** es el sector con más probabilidades de sufrir extorsiones (13 %).

La **sanidad**, como hemos visto, sufre un número de ataques inferior a la media. Sin embargo, los atacantes consiguen cifrar archivos en casi dos tercios (65 %) de los incidentes, lo que está considerablemente por encima de la media.

## Más víctimas están pagando el rescate

Preguntamos a las empresas cuyos datos fueron cifrados (1086) si recuperaron sus datos y, en caso afirmativo, cómo lo lograron.

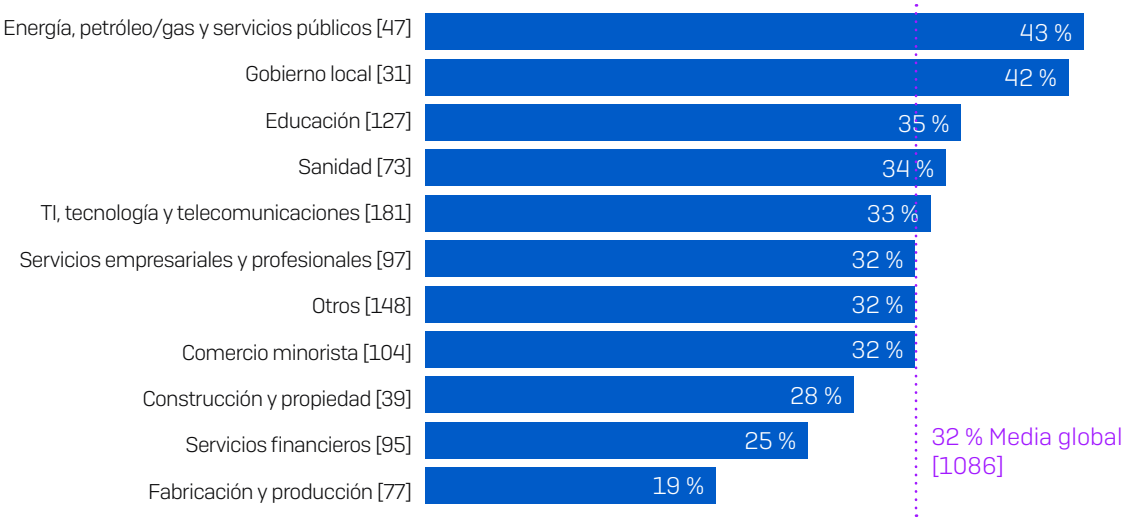
| 2020 | 2021 | |
|---|---|---|
| 26 % | 32 % | Pagaron el rescate para recuperar datos |
| 56 % | 57 % | Usaron copias seguridad para recuperar datos |
| 12 % | 8 % | Usaron otros medios para recuperar datos |
| 94 % | 96 % | Total de empresas que recuperaron sus datos |

*Nota: por motivos de redondeo, algunos totales no se corresponden con la suma de las cifras individuales*
*¿Su empresa recuperó los datos en el ataque de ransomware más importante?*
*[2021=1086, 2020=1849] empresas cuyos datos habían sido cifrados*

Como puede ver en el gráfico de arriba, el 32 % de las empresas pagaron el rescate para recuperar los datos, un incremento del 26 % con respecto a la encuesta del año anterior. El 57 % pudieron utilizar copias de seguridad para restaurar sus datos, lo que coincide con los resultados del año anterior. En términos generales, casi todas las empresas (96 %) pudieron recuperar algunos de sus datos.

## La predisposición a pagar varía por sector

También hay una diferencia considerable en el pago de los rescates entre sectores.




*¿Su empresa recuperó los datos en el ataque de ransomware más importante? Sí, pagamos el rescate; [número base en el gráfico] empresas en que los ciberdelincuentes lograron cifrar sus datos en el ataque de ransomware más importante, omitiendo algunas opciones de respuesta, divididas por sector*

El sector de la **energía, petróleo/gas y servicios públicos** es el más propenso a pagar el rescate, ya que el 43 % de los encuestados de estas empresas accedieron al pago de un rescate. Este sector suele tener mucha infraestructura heredada que no puede actualizarse fácilmente, de modo que las víctimas podrían sentirse obligadas a pagar el rescate a fin de permitir la continuidad de los servicios.

El **gobierno local** es el sector con el segundo nivel más alto de pagos de rescates (42 %). Curiosamente, esto sigue la línea del resultado anterior de que el gobierno local es el sector con más probabilidades de que se cifren sus datos. Es muy posible que la predisposición de las entidades de gobiernos locales a pagar esté provocando que los delincuentes dirijan sus ataques más complejos y efectivos contra este colectivo.

Parece que existe una relación entre la capacidad de una empresa para restaurar datos a partir de copias de seguridad y la probabilidad de que pague el rescate. La **fabricación y producción** es el sector con menos probabilidades de pagar el rescate y también el sector con más capacidad para restaurar datos a partir de copias de seguridad (68 %). De forma similar, la **construcción y propiedad**, así como los **servicios financieros**, muestran unos niveles inferiores a la media en pagos de rescates y una capacidad superior a la media para restaurar sus datos a partir de copias de seguridad.

El sector del **gobierno central y entidades públicas independientes** se ha excluido de este gráfico porque la base es demasiado reducida como para ser estadísticamente relevante. Anecdóticamente, de las 23 organizaciones de este sector cuyos datos fueron cifrados, el 61 % afirmaron que pudieron restaurar datos a partir de copias de seguridad y solo el 26 % pagaron el rescate. Este sugerente resultado podría ayudar a explicar por qué este sector es especialmente susceptible a los ataques de tipo extorsión.

### Pagar el rescate solo permite recuperar parte de los datos

**65 %**

**de datos restaurados después de pagar el rescate**

*Cantidad media de datos que recuperaron las empresas en el ataque de ransomware más importante; [344] empresas que pagaron el rescate para recuperar sus datos*

Lo que los atacantes no mencionan al exigir un rescate es que, aunque pague, las probabilidades de que recupere todos sus datos son escasas. De media, las empresas que pagaron el rescate recuperaron solo el 65 % de los archivos cifrados, de modo que más de un tercio de sus datos quedaron inaccesibles. El 29 % de los encuestados informaron de que el 50 % o menos de sus datos fueron restaurados, y solo el 8 % recuperaron todos sus datos.

## El coste del ransomware

### Los pagos de rescates varían enormemente

De los 357 encuestados que afirmaron que su empresa había pagado el rescate, 282 también revelaron el importe exacto pagado. Dentro de este grupo, el **pago medio fue de 170 404 USD**. Sin embargo, el abanico de las cuantías de los rescates es realmente amplio. El pago más común fue de 10 000 USD (pagado por 20 encuestados) y, el más alto, una astronómica cifra de 3,2 millones de USD (pagada por dos encuestados).

Estas cifras divergen mucho de los pagos de ocho cifras en USD que suelen verse en los titulares por varias razones.

1. **Tamaño de la empresa.** Nuestros encuestados son pequeñas y medianas empresas de entre 100 y 5000 usuarios que, en general, tienen menos recursos financieros que las empresas de mayor tamaño. Los responsables del ransomware adaptan los rescates que exigen a la capacidad de pago de sus víctimas, por lo que normalmente aceptan importes menores de empresas más pequeñas. Los datos lo demuestran, ya que el rescate medio para empresas de 100 a 1000 empleados fue de 107 694 USD, mientras que el rescate medio pagado por las empresas de 1001 a 5000 empleados ascendió a 225 588 USD.
2. **Tipo de ataque.** Hay muchos responsables del ransomware y muchos tipos de ataques de ransomware, desde atacantes altamente cualificados que utilizan tácticas, técnicas y procedimientos (TTP) sofisticados que se centran en objetivos individuales, hasta operadores menos habilidosos que utilizan ransomware "listo para usar" y un enfoque genérico de ataque "a ciegas". Los atacantes que realizan una gran inversión en un ataque dirigido exigen un elevado rescate que compense su esfuerzo, mientras que los responsables de ataques genéricos suelen aceptar un menor retorno de la inversión (ROI).
3. **Ubicación.** Los atacantes exigen los rescates más altos en economías occidentales desarrolladas, basándose en su percepción de que pueden pagar sumas mayores. Los dos importes de rescate más elevados fueron mencionados por encuestados de Italia.  Además, el rescate medio en todo EE. UU., Canadá, el Reino Unido, Alemania y Australia fue de 214 096 USD, que es un 26 % más alto que la media mundial (base: 101 encuestados). En cambio, en la India, el rescate medio fue de 76 619 USD, menos de la mitad de la cifra global (base: 86 encuestados).

## El coste de remediación del ransomware se ha duplicado con creces desde el año pasado

Pagar el rescate es solo una parte del coste de remediar un ataque. Si bien tanto el número de ataques de ransomware como el porcentaje de ataques en que los adversarios lograron cifrar los datos han disminuido desde el pasado año, el coste total de remediación de un ataque de ransomware ha aumentado.

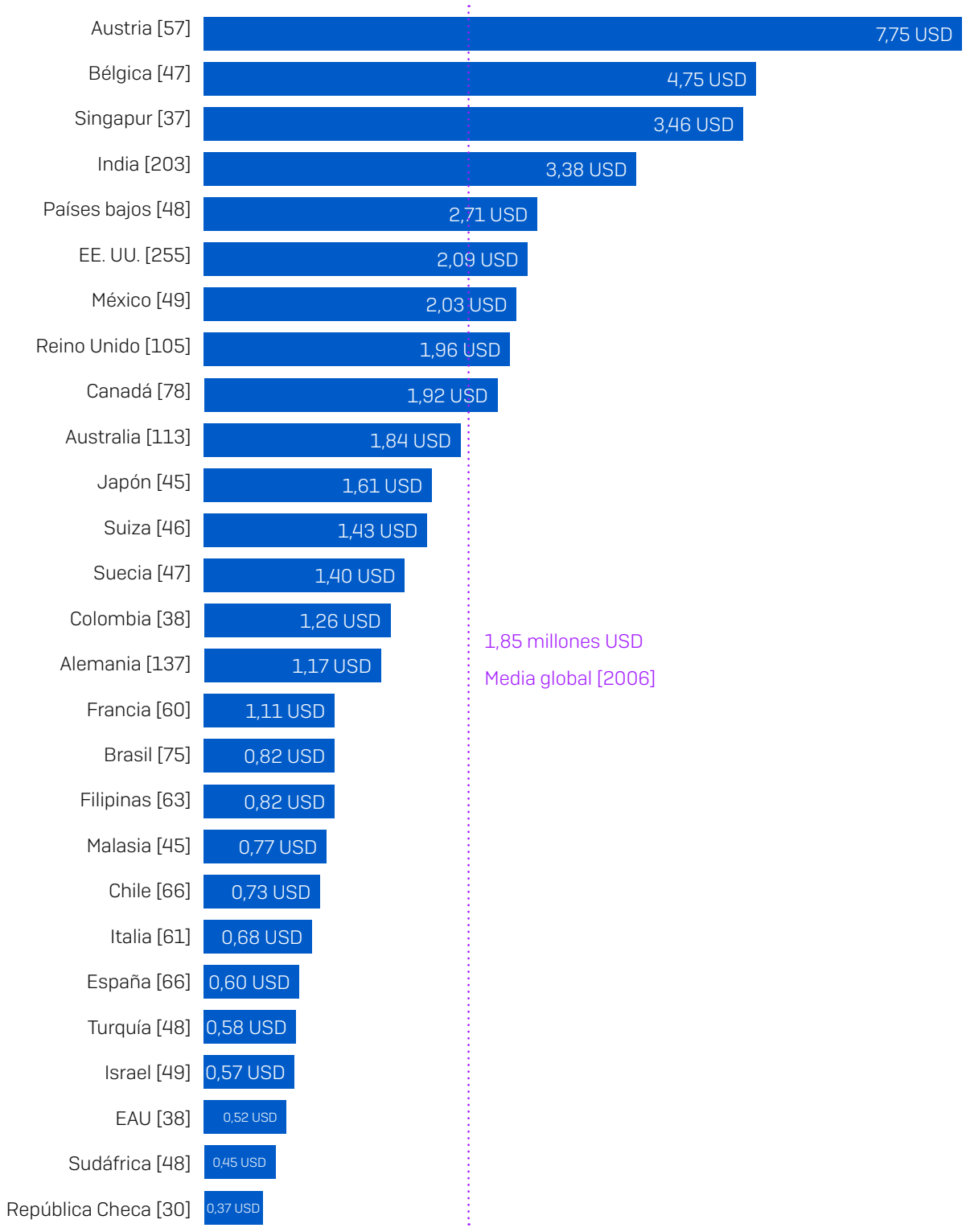
Los encuestados informaron de que el coste medio de rectificar las consecuencias del ataque de ransomware más reciente (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, etc.) fue de 1,85 millones USD, más del doble del coste de 761 106 USD registrado el año anterior.


*Coste medio aproximado para las empresas de rectificar las consecuencias del ataque de ransomware más reciente (considerando el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, etc.); [2021=2006, 2020=2538] encuestados cuya empresa se había visto afectada por el ransomware en el último año, divididas por año*

En el último año, los expertos en ransomware de Sophos han observado un considerable aumento de los ataques de ransomware avanzados que combinan la automatización con el hacking humano manual. Estos ataques complejos requieren procesos de recuperación más complejos, y esto podría ser un factor clave para explicar el incremento general de los costes de recuperación del ransomware.

## Los costes de remediación varían en función de la ubicación

Si miramos los costes de remediación del ransomware por países, vemos importaciones variaciones.




*Coste medio aproximado para las empresas de rectificar las consecuencias del ataque de ransomware más reciente [considerando el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, etc.]; [números base en el gráfico] encuestados cuya empresa se había visto afectada por el ransomware en el último año, divididas por país, millones de USD*

Austria destaca como el país con el coste de remediación del ransomware más elevado. En el último año se han producido varios ciberataques de alto perfil contra organizaciones austríacas, entre ellas el ministerio de asuntos exteriores de Austria, que supuestamente sufrió un ataque de un agente estatal, además de que el grupo de ransomware Netwalker afirmó en Twitter haber robado datos a la ciudad austríaca de Weiz. Cabe señalar que, si excluimos a Austria de los datos, el coste medio de remediación solo baja hasta los 1,68 millones USD, que sigue siendo más del doble de la cifra del año previo.

En general, en países con salarios superiores (Bélgica, Singapur, los Países Bajos y los EE. UU.) se registran los costes generales más altos, mientras que los países con salarios inferiores (República Checa y Sudáfrica) registran los costes generales más bajos. Esto refleja el considerable esfuerzo manual que se necesita para remediar un ataque. Efectivamente, el coste total de remediar un ataque de ransomware es diez veces superior al pago del rescate medio.

Israel se encuentra entre los países con unos costes generales de remediación de ransomware más bajos a pesar de tratarse de una economía desarrollada. Por motivos geopolíticos, Israel es uno de los principales blancos de los ciberataques (no solo de ransomware), lo que se traduce en unos niveles muy altos de ciberdefensas, preparación y experiencia en remediación en todo el país. La combinación de estos factores rebaja el impacto financiero de un ataque.

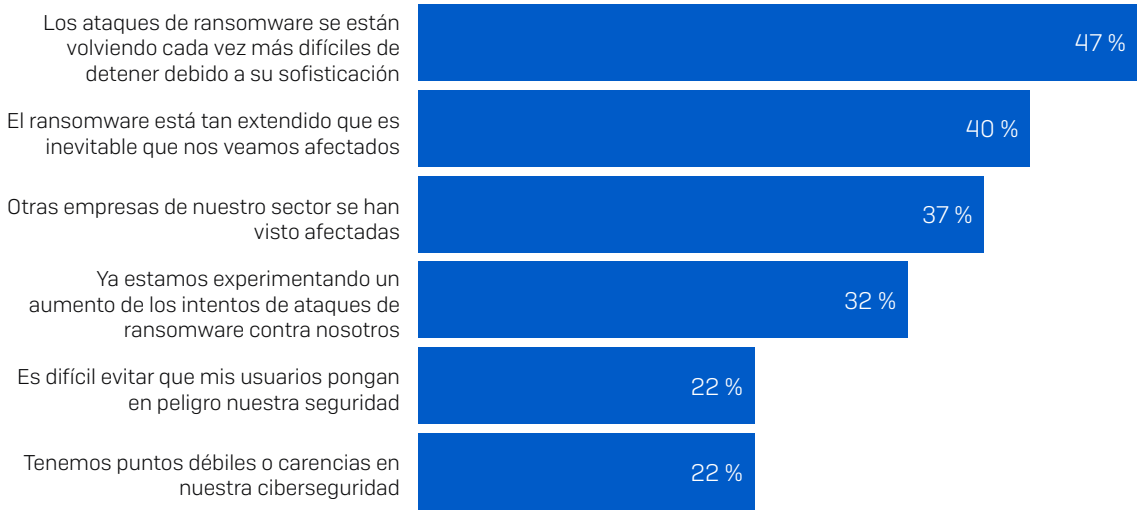
# El futuro

## Las expectativas con respecto a los ataques de ransomware varían

El 62 % de los encuestados (3353) afirmaron que su empresa no había sufrido ataques de ransomware en el último año. Dentro de este grupo, observamos variaciones importantes en cuanto a su actitud hacia el ransomware y a su confianza en poder en gestionarlo. El 65 % de los encuestados esperan ataques de ransomware en el futuro, mientras que el 35 % no prevén ninguno.

## Por qué esperan ataques de ransomware las empresas

Entre los 2187 encuestados de empresas que no fueron víctimas del ransomware en el último año pero que esperan serlo en el futuro, la razón más común por la que esperan sufrir un ataque es que "los ataques de ransomware se están volviendo cada vez más difíciles de detener debido a su sofisticación", en palabras del 47 % de los encuestados de este grupo.



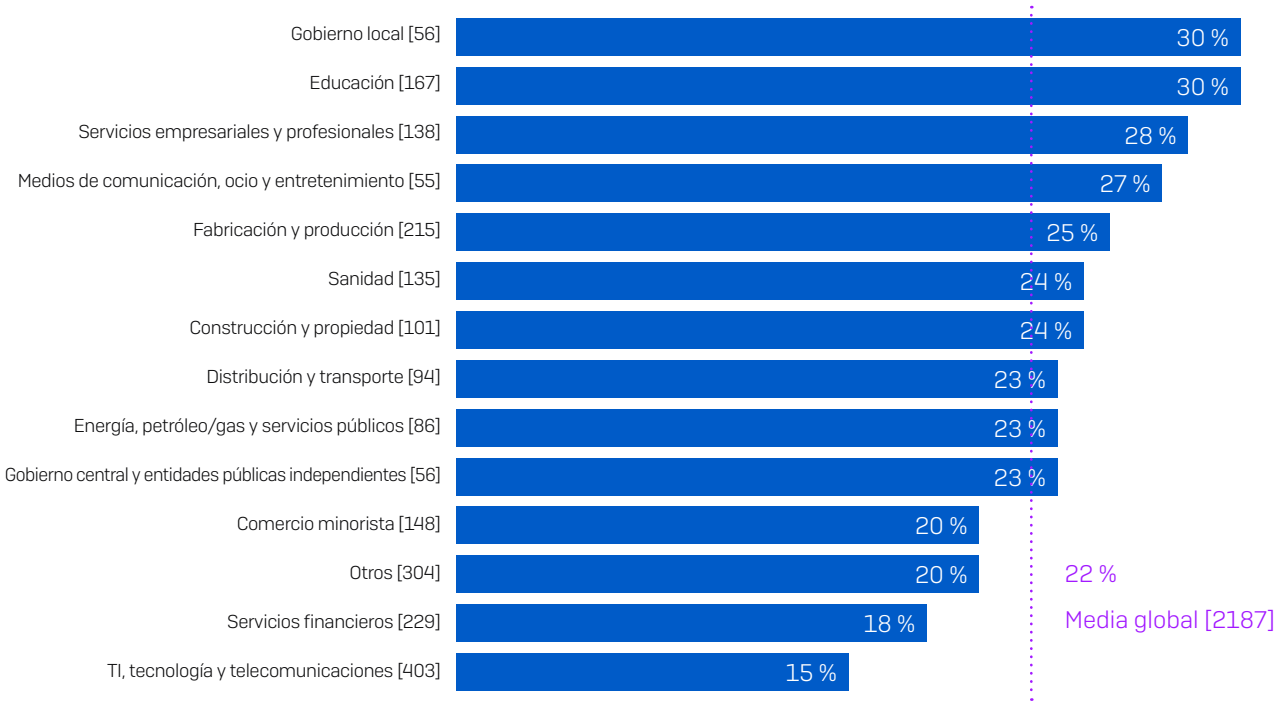

*¿Por qué espera que su empresa sea atacada por el ransomware en el futuro? [2187] empresas que no fueron atacadas por el ransomware en el último año pero que esperan serlo en el futuro, omitiendo algunas opciones de respuesta*

Aunque este número es elevado, el hecho de que estas empresas estén alerta ante la posibilidad de que el ransomware se vuelva más avanzado es algo positivo, y es probable que sea un factor que ha contribuido a que hayan podido bloquear cualquier posible ataque de ransomware durante el último año.

El 22 % de los encuestados ven el hecho de que los usuarios comprometan la seguridad como uno de los principales factores para sufrir un ataque de ransomware en el futuro. Resulta alentador observar que, frente a los atacantes sofisticados, la mayoría de los equipos de TI no eligen la opción fácil de culpar a sus usuarios.

De forma similar, el 22 % de los encuestados admiten tener puntos débiles o carencias en su ciberseguridad. Aunque lógicamente no es buena idea tener brechas de seguridad, reconocer estos problemas es un importante primer paso para mejorar las defensas.

Si profundizamos en este aspecto, vemos que los sectores del gobierno local y la educación son los que más probabilidades tienen de admitir que sufren carencias (el 30 % cada uno).




*¿Por qué espera que su empresa sea atacada por el ransomware en el futuro? Tenemos puntos débiles o carencias en nuestra ciberseguridad; [números base en el gráfico] empresas que no fueron atacadas por el ransomware en el último año pero que esperan serlo en el futuro, omitiendo algunas opciones de respuesta, divididas por sector*

Aunque los que respondieron a esta pregunta no sufrieron ellos mismos ningún ataque de ransomware en el último año, es probable que les hayan influido las experiencias generales con el ransomware en sus sectores:

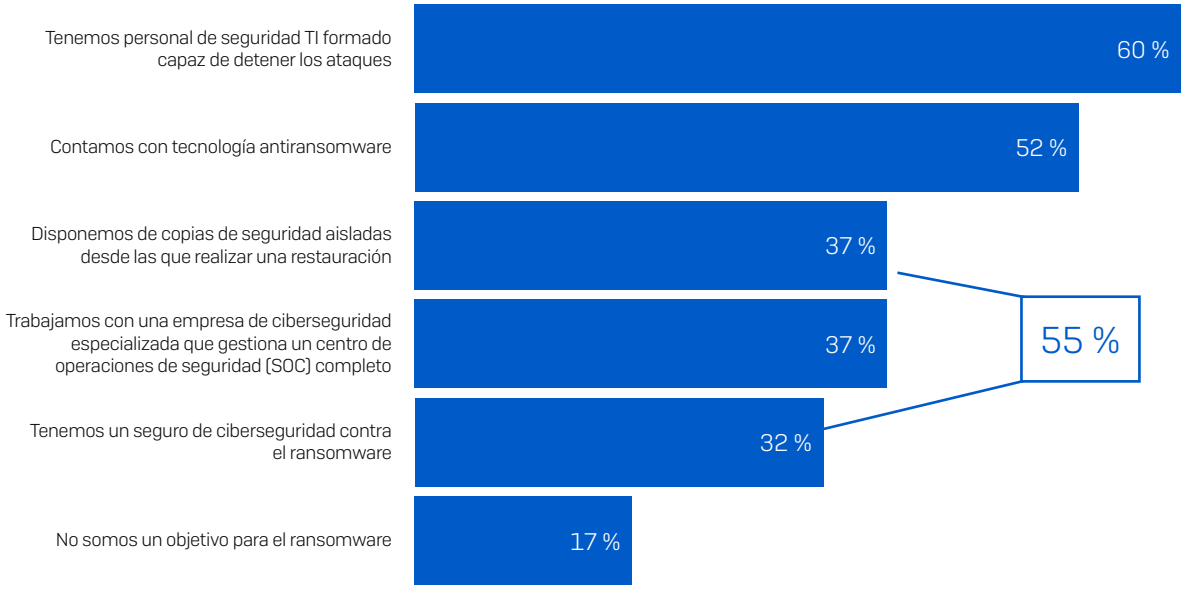
- El **gobierno local** es el sector en el que los atacantes tienen más probabilidades de llegar a cifrar los datos de la víctima.
- La **educación** (junto con el comercio minorista) es el sector que registró el mayor porcentaje de organizaciones afectadas por el ransomware en el último año.

Asimismo, ambos sectores suelen tener problemas de financiación tanto para tecnología como para recursos de TI, lo que también se traduce en brechas de seguridad.

En cambio, las **TI, telecomunicaciones y tecnología** (15 %) y los **servicios financieros** (18 %) tienen el porcentaje más bajo de encuestados que admiten sufrir carencias de seguridad. Estos son sectores que, en general, adoptan nuevas tecnologías rápidamente y disponen de mayores presupuestos, de modo que tienen más oportunidades para resolver las deficiencias.

## El personal de TI formado da confianza frente al ransomware

1166 encuestados dijeron que no habían sufrido ataques de ransomware en el último año y que no esperan sufrir ninguno en el futuro. El principal motivo de esta confianza frente al ransomware es contar con personal de TI formado capaz de detener los ataques.




*¿Por qué no espera que su empresa sea atacada por el ransomware en el futuro? [1166] empresas que no fueron atacadas por el ransomware en el último año y que no esperan serlo en el futuro, omitiendo algunas opciones de respuesta*

Si bien las tecnologías avanzadas y automatizadas son elementos fundamentales de una defensa antiransomware efectiva, detener los ataques manuales también requiere una monitorización e intervención humanas por parte de profesionales cualificados. Ya sean empleados en plantilla o profesionales subcontratados, solo los expertos humanos pueden identificar algunos de los indicios de que los atacantes del ransomware le tienen en el punto de mira.

El 37 % de los encuestados que no esperan ser atacados por el ransomware trabajan con una empresa de ciberseguridad especializada que gestiona un centro de operaciones de seguridad (SOC) completo. Hace tan solo unos años, los SOC estaban al alcance exclusivamente de las grandes compañías, por lo que esto representa un gran cambio en la prestación de servicios de ciberseguridad a medianas empresas.

No todo son buenas noticias. Algunos resultados son preocupantes:

- El 55 % de los encuestados que no esperan sufrir ningún ataque depositan su confianza en enfoques que no ofrecen ninguna protección contra el ransomware:
  - El 37 % de los encuestados citaron las "copias de seguridad aisladas" como motivo por el que no esperan ser atacados. Las copias de seguridad, como hemos visto, son herramientas valiosas para restaurar los datos después de un ataque, pero no evitan el ataque en sí.

- El 32 % de los encuestados afirmaron que contar con un seguro de ciberseguridad les protege de los ataques de ransomware. De nuevo, un seguro puede ser de gran ayuda en la etapa posterior a un ataque, pero no evita que este se produzca.

**N. B. Algunos encuestados seleccionaron ambas opciones, y el 55 % seleccionaron al menos una de estas dos opciones.**

- Asimismo, el 17 % de los encuestados no creen que sean el objetivo del ransomware. Lamentablemente, esto no es así. Ninguna organización está a salvo.

## Los planes de recuperación ante incidentes de malware son la norma

Responder a un ciberataque o incidente crítico puede ser increíblemente estresante. Aunque nada puede aliviar por completo el estrés que supone lidiar con un ataque, contar con un plan de respuesta a incidentes efectivo es una forma segura de minimizar el impacto.

Por esta razón, resulta alentador descubrir que el 90 % de los encuestados afirman que su empresa cuenta con un plan de recuperación de incidentes de malware: un poco más de la mitad (51 %) tiene un plan completo y detallado, mientras que el 39 % tiene un plan parcialmente desarrollado.

Existen muchos paralelismos entre recuperarse del malware y recuperarse de un desastre natural, ya que en ambos escenarios hay que tener la capacidad de empezar de nuevo desde cero. Las Filipinas, un país que sufre frecuentes inundaciones y terremotos, es el más preparado para hacer frente a un incidente de malware, ya que un 83 % de los encuestados afirmaron contar con un plan de recuperación de incidentes de malware completo y detallado.

## Las organizaciones gubernamentales son las menos preparadas para responder a un ataque de malware

Muchos sectores están bien preparados para recuperarse de un incidente de malware. Sin embargo, las organizaciones gubernamentales han demostrado ser las menos preparadas: solo el 73 % del **gobierno local** y el 81 % del **gobierno central y entidades públicas independientes** cuentan con un plan de recuperación.

Esto es preocupante, puesto que estos sectores son de los más afectados por el ransomware. El gobierno local es el sector con más probabilidades de que se cifren sus datos en un ataque, mientras que el gobierno central y entidades públicas independientes son los que más probabilidades tienen de sufrir extorsiones.

La falta de un plan de recuperación del malware podría ser uno de los factores que contribuyen a que el gobierno local sea el segundo sector con más probabilidades de pagar los rescates exigidos.

# Recomendaciones

En vista de estos resultados, los expertos de Sophos recomiendan aplicar estas prácticas:

1. **Dé por hecho que sufrirá un ataque.** El ransomware sigue estando muy extendido. No hay ningún sector, país ni organización a salvo del riesgo. Es mejor prepararse y no sufrir ningún ataque que lo contrario.

2. **Realice copias de seguridad.** Las copias de seguridad son el principal método utilizado por las empresas para recuperar sus datos tras un ataque. Y como ya hemos visto, incluso si paga el rescate, rara vez conseguirá recuperar todos sus datos, así que depende de las copias de seguridad en cualquiera de los casos.

3. **Despliegue una protección por capas.** Ante el importante aumento de los ataques basados en la extorsión, es más importante que nunca mantener a los adversarios fuera de su entorno como primera medida. Utilice una protección por capas para bloquear a los atacantes en tantos puntos como sea posible dentro de su entorno.

4. **Combine expertos humanos y tecnología antiransomware.** Una de las claves para detener el ransomware es una defensa exhaustiva que combine una tecnología antiransomware dedicada y la búsqueda de amenazas realizada por humanos. La tecnología le brinda el alcance y la automatización que necesita, mientras que los expertos humanos están más capacitados para detectar las tácticas, técnicas y procedimientos que indican que un atacante habilidoso está intentando infiltrarse en su entorno. Si no dispone de las habilidades internamente, plantéese la opción de solicitar el apoyo de una empresa de ciberseguridad especializada: hoy en día los SOC son una opción realista para las empresas de todos los tamaños.

5. **No pague el rescate.** Sabemos que esto es fácil de decir pero mucho menos fácil de hacer cuando la actividad de su empresa se encuentra interrumpida a causa de un ataque de ransomware. Con independencia de cualquier consideración ética, pagar el rescate no es una forma efectiva de recuperar sus datos. Si opta por pagar, asegúrese de incluir en su análisis de costes y beneficios la expectativa de que los adversarios restaurarán, de media, solo dos terceras partes de sus archivos.

6. **Tenga un plan de recuperación del malware.** La mejor manera de evitar que un ciberataque acabe en una infracción de seguridad es prepararse con antelación. Las empresas que sufren un ataque a menudo se dan cuenta de que podrían haber evitado muchos costes, molestias e interrupciones si hubieran contado con un plan de respuesta a incidentes.

## Más recursos

La Guía de respuesta a incidentes de Sophos ayuda a las empresas a definir el marco de su plan de respuesta a incidentes de ciberseguridad y explica los 10 principales pasos que debe incluir su plan.

A los responsables de la seguridad también puede interesarles consultar el artículo Cuatro consejos clave de los expertos en respuesta a incidentes, que pone de relieve las principales lecciones que todo el mundo debería aprender en lo que respecta a responder a incidentes de seguridad.

Ambos recursos se basan en experiencias del mundo real de los equipos de Sophos Managed Threat Response y Sophos Rapid Response, que han respondido de forma conjunta a miles de incidentes de ciberseguridad.

Obtenga más información sobre el ransomware y cómo Sophos puede ayudarle a proteger su empresa.

Sophos ofrece soluciones de ciberseguridad líderes en la industria a empresas de todos los tamaños a fin de protegerlas 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 empresa estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.



19-04-2021 (SB-NP)

SOPHOS