SOPHOS
Cybersecurity delivered.

El estado del ransomware 2022

Resultados de una encuesta independiente y desvinculada de cualquier proveedor a 5600 profesionales de TI de organizaciones de tamaño medio en 31 países.

Monográficos de Sophos. Abril de 2022

Introducción

El estudio anual de Sophos sobre las experiencias reales con ransomware de los profesionales de TI que trabajan en primera línea ha revelado la existencia de un entorno hostil cada vez más desafiante, además de la creciente carga, tanto a nivel financiero como operativo, a la que el ransomware está sometiendo a sus víctimas. También arroja nueva luz sobre la relación entre el ransomware y los ciberseguros, y el papel que desempeñan estos para impulsar cambios en las ciberdefensas.

Acerca de la encuesta

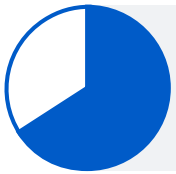
Sophos encargó a la empresa de investigación especializada Vanson Bourne la realización de una encuesta independiente y desvinculada de cualquier proveedor a 5600 profesionales de TI en organizaciones de tamaño medio (100-5000 empleados) de 31 países. La encuesta se realizó durante enero y febrero de 2022 y a los encuestados se les pidió contestar según sus experiencias del año anterior.

Los ataques aumentan con una complejidad y un impacto cada vez mayores

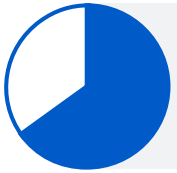
El año pasado se vieron afectadas por el ransomware el 66 % de las organizaciones encuestadas, mientras que en 2020 fueron el 37 %. Esto representa un incremento del 78 % en el transcurso de un año, lo que demuestra que los adversarios se han vuelto considerablemente más capaces de ejecutar los ataques más importantes a escala. Este incremento probablemente también refleje el creciente éxito del modelo de ransomware como servicio, que amplía significativamente el alcance del ransomware al requerir menos conocimientos para ejecutar los ataques. [Nota: por organización afectada por el ransomware se entiende uno o más dispositivos afectados por un ataque, pero sin implicar necesariamente su cifrado.]

Los adversarios también se han vuelto más eficaces a la hora de cifrar los datos en sus ataques. En 2021 los atacantes lograron cifrar los datos en el 65 % de los ataques, lo que supone un aumento respecto al índice de cifrado del 54 % en 2020. Sin embargo, se ha producido una reducción del 7 % al 4 % en el porcentaje de las víctimas que sufrieron ataques de solo extorsión, en los que los datos no fueron cifrados pero sí se exigió un rescate con la amenaza de divulgar los datos.

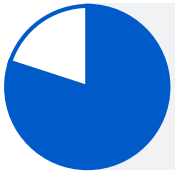
El aumento del éxito de los ataques de ransomware forma parte de un entorno de amenazas cada vez más amplio y desafiante: durante el último año, el 57 % de las organizaciones encuestadas experimentó un aumento del volumen de los ciberataques en general, el 59 % vio aumentar la complejidad de los ataques y el 53 % afirmó que había aumentado el impacto de los ataques. El 72 % apreció un aumento en por lo menos una de estas áreas.



66 %
afectadas por el ransomware en el último año



65 %
ataques conllevaron el cifrado de datos



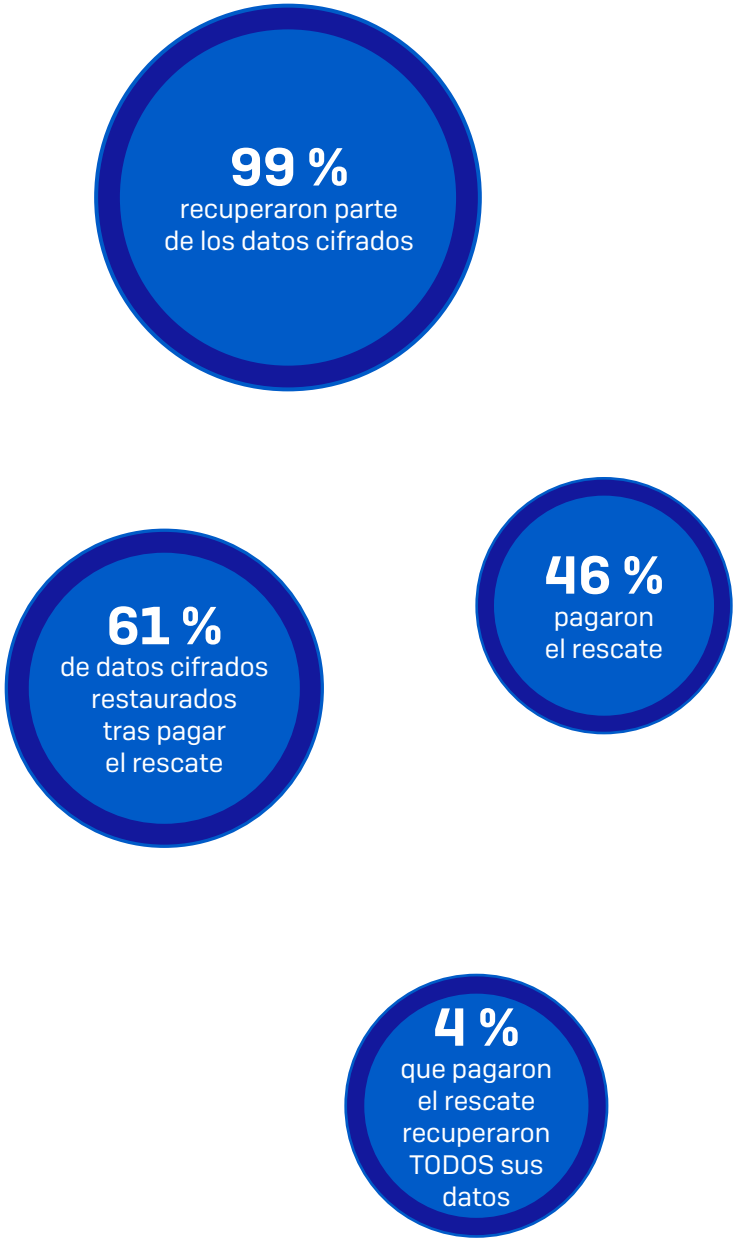
72 %
experimentaron un aumento en el volumen/complejidad/ impacto de los ciberataques

Las organizaciones están mejorando a la hora de restaurar los datos después de un ataque

A medida que el ransomware se ha vuelto más frecuente, las organizaciones han mejorado en lo que respecta a solventar las secuelas de un ataque. Casi todas las organizaciones afectadas por el ransomware durante el último año (99 %) consiguieron recuperar parte de los datos cifrados, lo que supone un ligero aumento en comparación con el 96 % del año anterior.

Las copias de seguridad son el principal método utilizado para restaurar los datos, usado por el 73 % de las organizaciones cuyos datos fueron cifrados. A su vez, un 46 % reveló haber pagado un rescate para restaurar sus datos. Estas cifras reflejan el hecho de que muchas organizaciones utilizan múltiples enfoques de restauración con el fin de maximizar la velocidad y la eficacia con la que reinician su actividad. En general, casi la mitad (44 %) de los encuestados cuyos datos corporativos habían sido cifrados recurrieron a múltiples métodos para restaurar sus datos.

Mientras que pagar el rescate casi siempre permite recuperar parte de los datos, el porcentaje de los datos restaurados después de pagar ha bajado. De media, las organizaciones que pagaron solo recuperaron el 61 % de sus datos, dato algo menor con respecto al 65 % de 2020. De forma similar, en 2021 solo el 4 % de los que pagaron un rescate recuperaron TODOS sus datos, de nuevo una reducción con respecto al 8 % de 2020.



Los pagos de rescates han aumentado

965 encuestados de organizaciones que pagaron el rescate revelaron la cifra exacta, lo que ha permitido constatar que este último año el importe medio de los pagos de rescate ha aumentado de forma importante.

Así, la proporción de víctimas que han pagado rescates de 1 millón USD o más se ha multiplicado casi por tres, subiendo del 4 % en 2020 al 11 % en 2021. Paralelamente, el porcentaje de víctimas que pagaron menos de 10 000 USD ha disminuido de una de cada tres (34 %) en 2020 a una de cada cinco (21 %) en 2021.

En general, la media de los rescates se situó en 812 360 USD, lo que supone 4,8 veces más con respecto a la media de 170 000 dólares del 2020 (basada en las respuestas de 282 encuestados). Aunque esta cifra está influenciada por 15 pagos de 8 dígitos, los datos claramente indican que los rescates tienden al alza en general. A su vez, se presentan variaciones considerables en función del sector, y los adversarios obtienen las sumas más altas de aquellos que consideran que tienen más capacidad para pagar:

- El promedio de pagos de rescate MÁS ALTO fue de 2,04 millones USD en el sector de la fabricación y producción (n=38) y de 2,03 millones USD en el de la energía, el petróleo/gas y los servicios públicos (n=91)
- El promedio de pagos de rescate MÁS BAJO fue de 197 000 USD en el sector sanitario (n=83) y de 214 000 USD en el sector de gobierno local/estatal (n=20)

En Italia, donde el pago de extorsiones es ilegal, es decir, que la legislación no permite que las organizaciones paguen rescates, el 43 % de los encuestados cuyos datos fueron cifrados admiten que su organización pagó un rescate (n=76). El estudio demuestra que las barreras legislativas por sí solas no son efectivas para detener el pago de rescates.

3x
aumento de la proporción que pagó rescates de más de 1 millón USD

21 %
pagaron rescates de menos de 10 000 USD

812 360 USD
media de los rescates (excl. casos atípicos)

FABRICANTES, SERVICIOS PÚBLICOS
pago de rescate medio más alto (2 millones USD)

SANIDAD
pago de rescate medio más bajo (197 000 USD)

El ransomware tiene un importante impacto comercial y operativo

Las sumas de los rescates son solo una parte de la historia, y el impacto del ransomware abarca mucho más que solo el cifrado de bases de datos y dispositivos. El 90 % de los afectados por el ransomware en el último año afirmó que el ataque más importante afectó su capacidad operativa. Es más, entre las organizaciones pertenecientes al sector privado, el 86 % indicó haber sufrido pérdidas de negocio/ingresos.

En general, el coste medio para que una organización subsane el impacto del ataque de ransomware más reciente en 2021 se situó en 1,4 millones USD. Esta bienvenida reducción con respecto a los 1,85 millones USD en 2020 probablemente sea reflejo de que, a medida que el ransomware se ha hecho más frecuente, ha disminuido el daño a la reputación de un ataque. Paralelamente, las aseguradoras están mejor capacitadas para guiar a las víctimas de forma rápida y efectiva a través del proceso de respuesta al incidente, lo que reduce los costes de remediación de los ataques.

Cabe reseñar que en muchos de los casos en los que se paga el rescate, dicho pago corre a cargo de la aseguradora y no de la víctima. Trataremos este tema con más detalle más adelante en este informe.

De media, las organizaciones que sufrieron ataques en el último año tardaron un mes en recuperarse del ataque más importante, mucho tiempo para la mayoría de empresas. Las recuperaciones más lentas se dieron en los sectores de educación superior y de gobierno central/federal, en los que dos de cada cinco organizaciones tardaron más de un mes en recuperarse. En cambio, los sectores más rápidos fueron el de la fabricación y producción (el 10 % tardó más de un mes) y el de los servicios financieros (el 12 % tardó más de un mes), seguramente como resultado de los elevados niveles de planificación y preparación para recuperarse de este tipo de incidentes.

Además, algunas organizaciones siguen depositando sus esperanzas en defensas ineficaces. De los encuestados cuyas organizaciones no fueron afectadas por el ransomware durante el último año y que tampoco esperan serlo en el futuro, el 72 % se basan en enfoques que no impiden que las organizaciones sean atacadas: entre las razones por las que no prevén un ataque, el 57 % mencionó las copias de seguridad y el 37 % citó los ciberseguros, habiendo algunos de ellos seleccionado ambas opciones. Aunque estos elementos sirvan de ayuda para recuperarse de un ataque, no lo evitan en primer lugar.

90 %
vieron afectada su capacidad operativa por un ataque de ransomware

86 %
sufrieron pérdidas de negocio/ingresos por un ataque de ransomware

1,4 millones USD
coste medio de remediación de un ataque

UN MES
tiempo medio de recuperación tras un ataque

72 %
confían en enfoques que no impiden un ataque

Las organizaciones son incapaces de usar sus presupuestos y recursos de forma efectiva para detener el ransomware

La encuesta ha constatado que afrontar el problema solo con personal y dinero no es la solución. Más bien es cuestión de invertir en la tecnología adecuada y disponer de los conocimientos y la experiencia necesarios para usarla de forma efectiva. En caso contrario, el retorno de la inversión es bajo.

El 64 % de los afectados por el ransomware en el último año afirma tener más presupuesto de ciberseguridad del que necesitan, mientras que otro 24 % indica que tener el presupuesto adecuado. De forma similar, el 65 % de las víctimas de ransomware piensan tener más personal de ciberseguridad del necesario y el 23 % piensa que el nivel de personal es suficiente. Estos resultados sugieren que muchas organizaciones tienen dificultades para desplegar sus recursos de forma efectiva frente al creciente volumen y la complejidad de los ataques.

Asimismo, los resultados también indican que posiblemente las organizaciones no sean conscientes de que no tienen los conocimientos adecuados para detener las técnicas de ataque más recientes: el 58 % de los afectados por el ransomware piensa que su organización monitoriza siempre/casi siempre los registros para detectar señales o actividades sospechosas, y el 56 % afirma que sus organizaciones están totalmente/mayormente al día de las herramientas/métodos de ataque más recientes.

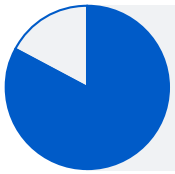
En cambio, entre las organizaciones no afectadas por el ransomware en el último año y que tampoco prevén ataques en el futuro, la principal razón detrás de esta confianza es disponer de un equipo de seguridad TI experimentado o un centro de operaciones de seguridad (SOC) interno capaz de detener los ataques.

El ransomware: motor de los ciberseguros

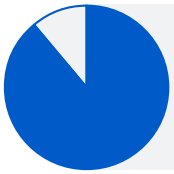
Más de cuatro de cada cinco organizaciones medianas tienen contratado un ciberseguro contra ransomware. Sin embargo, mientras que el 83 % de los encuestados confirman que su organización cuenta con un ciberseguro que les cubre en caso de verse afectados por el ransomware, el 34 % afirman que la póliza contiene exclusiones/excepciones. Los sectores de energía, petróleo/gas y servicios públicos son los que más seguros contratan (89 %), seguidos de cerca por el sector del comercio minorista (88 %). La contratación de ciberseguros aumenta con el tamaño de la organización: dentro de las organizaciones con 3001-5000 empleados, la contratación de pólizas alcanza un porcentaje del 88 %, frente al 73 % en las organizaciones con 100-250 empleados.

Las organizaciones afectadas por el ransomware en el último año son mucho más propensas a tener contratado un ciberseguro que aquellas que han evitado ser víctimas de un ataque. Entre las afectadas, un 89 % tiene un ciberseguro, mientras que entre las que no se han visto afectadas, el porcentaje es del 70 %. Aquí la relación de causa y efecto no está clara. Puede ser que la experiencia directa de un incidente de ransomware haya llevado a muchas organizaciones a contratar un seguro para ayudar a mitigar el impacto de ataques futuros. Por otro lado, los adversarios pueden atacar a organizaciones que saben que tienen un seguro para aumentar sus probabilidades de cobrar un rescate. Otra opción es que algunas organizaciones contraten un seguro para compensar las debilidades manifiestas en sus defensas. La realidad seguramente sea una combinación de las tres.

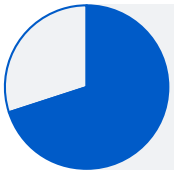
Entre las organizaciones que no se han visto afectadas por el ransomware ni tampoco esperan sufrir un ataque, el porcentaje de las que cuentan con un seguro baja hasta el 61 %. Dado que muchas de las organizaciones de este grupo confían en enfoques que no detienen el ransomware, la falta de cobertura las deja completamente expuestas a los costes de un incidente.



83 %
disponen de un ciberseguro contra ransomware



89 %
de afectados por el ransomware disponen de un ciberseguro



70 %
de no afectados por el ransomware disponen de un ciberseguro

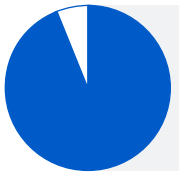
Los ciberseguros propician la mejora de las ciberdefensas

El 94 % de las organizaciones con un ciberseguro contratado afirmaron que el proceso de obtención de la cobertura había cambiado en el último año.

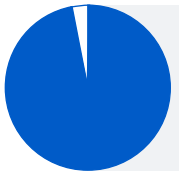
- Según el 54 %, el nivel de ciberseguridad necesario para optar a un seguro ahora es más alto
- Según el 47 %, las pólizas ahora son más complejas
- Según el 40 %, el número de empresas que ofrecen ciberseguros se ha reducido
- Según el 37 %, el proceso es más largo
- Según el 34 %, es más caro

Dado que la subidas de precio más importantes de los ciberseguros se produjeron durante el segundo y el tercer trimestre de 2021, es probable que muchos de los encuestados todavía no hubiesen sufrido el impacto de este cambio en las fechas de la encuesta.

A medida que el mercado de los ciberseguros se endurece y cada vez es más difícil hacerse con un seguro, el 97 % de las organizaciones con un ciberseguro han introducido cambios en su ciberdefensa para mejorar su posición frente a las aseguradoras. Un 64 % ha implementado tecnologías/servicios nuevos, un 56 % ha incrementado las actividades de formación/capacitación de su personal y un 52 % ha cambiado procesos/conductas.



94 %
han encontrado más dificultades para contratar un ciberseguro en el último año



97 %
de los que tienen un ciberseguro han introducido cambios en sus defensas para mejorar su posición frente a las ciberaseguradoras

Los ciberseguros pagan en casi todas las reclamaciones por ransomware

De manera tranquilizadora para aquellas organizaciones que están aseguradas, el 98 % de los afectados por el ransomware y que contaban con un seguro que cubría el ransomware indicó que la póliza les indemnizó por el ataque más importante, lo que supone un incremento frente al 95 % en 2019. En algunos países este porcentaje aumentó hasta alcanzar el 100 %: Suiza (n=52), México (n=131), Suecia (n=68), Bélgica (n=66), Polonia (n=75), Turquía (n=51), EAU (n=49), India (n=218) y Singapur (n=91).

Analizando lo que pagó la cobertura de ciberseguridad, la encuesta revela un aumento en el pago de los costes de limpieza y un descenso en los pagos de rescates por parte de las aseguradoras. El 77 % de los encuestados informó de que su aseguradora pagó los costes de limpieza, es decir, los costes incurridos para que la organización recuperara su actividad, lo que representa una subida frente al 67 % de 2019. En cambio, en lo que respecta al pago de rescates por parte de la compañía aseguradora, se experimentó una bajada, un 40 % en comparación con un 44 % en 2019.

Sin embargo, hay que tener en cuenta que el pago de rescates varía considerablemente en función del sector. Los porcentajes más altos corresponden a los sectores de la educación (primaria/secundaria) (53 %), el gobierno local/estatal (49 %) y la sanidad (47 %), y los más bajos a la fabricación y producción (30 %) y los servicios financieros (32 %). Es interesante reseñar que los sectores con las tasas de pago de rescates más bajas también son aquellos capaces de recuperarse en menos tiempo, lo que enfatiza la importancia que tiene la preparación y disponer de un plan de recuperación de desastres.

Cabe recordar que, aunque un ciberseguro le ayudará a restaurar el estado anterior, no cubre la mejora, es decir, la inversión en tecnologías y servicios mejores para subsanar las debilidades que condujeron al ataque.

98 %
tasa de pago de indemnizaciones por ransomware

△ Pago de los costes de limpieza △

2019	2021
67 %	77 %

▽ Pago del rescate ▽

2019	2021
44 %	40 %

Conclusión

El desafío que el ransomware representa para las organizaciones no deja de crecer. La proporción de organizaciones impactadas directamente por el ransomware prácticamente se ha duplicado en doce meses: de algo más de un tercio en 2020 a dos tercios en 2021.

En vista de esta casi normalización, las organizaciones han mejorado en lo que respecta a solventar las secuelas de un ataque: prácticamente todas recuperan parte de los datos cifrados y casi tres cuartas partes son capaces de usar las copias de seguridad para restaurar sus datos.

A su vez, de media, la proporción de datos cifrados recuperados tras pagar un rescate ha bajado a un 61 %. A pesar de esto, el porcentaje de las víctimas que han pagado rescates de 1 millón USD o más casi se ha triplicado.

La encuesta ha constatado que afrontar el problema solo con personal y dinero no es la solución. Más bien es cuestión de invertir en la tecnología adecuada y disponer de los conocimientos y la experiencia necesarios para usarla de forma efectiva. Las organizaciones deben recurrir a expertos que puedan ayudarles a mejorar el retorno de sus inversiones en ciberseguridad y aumentar sus defensas.

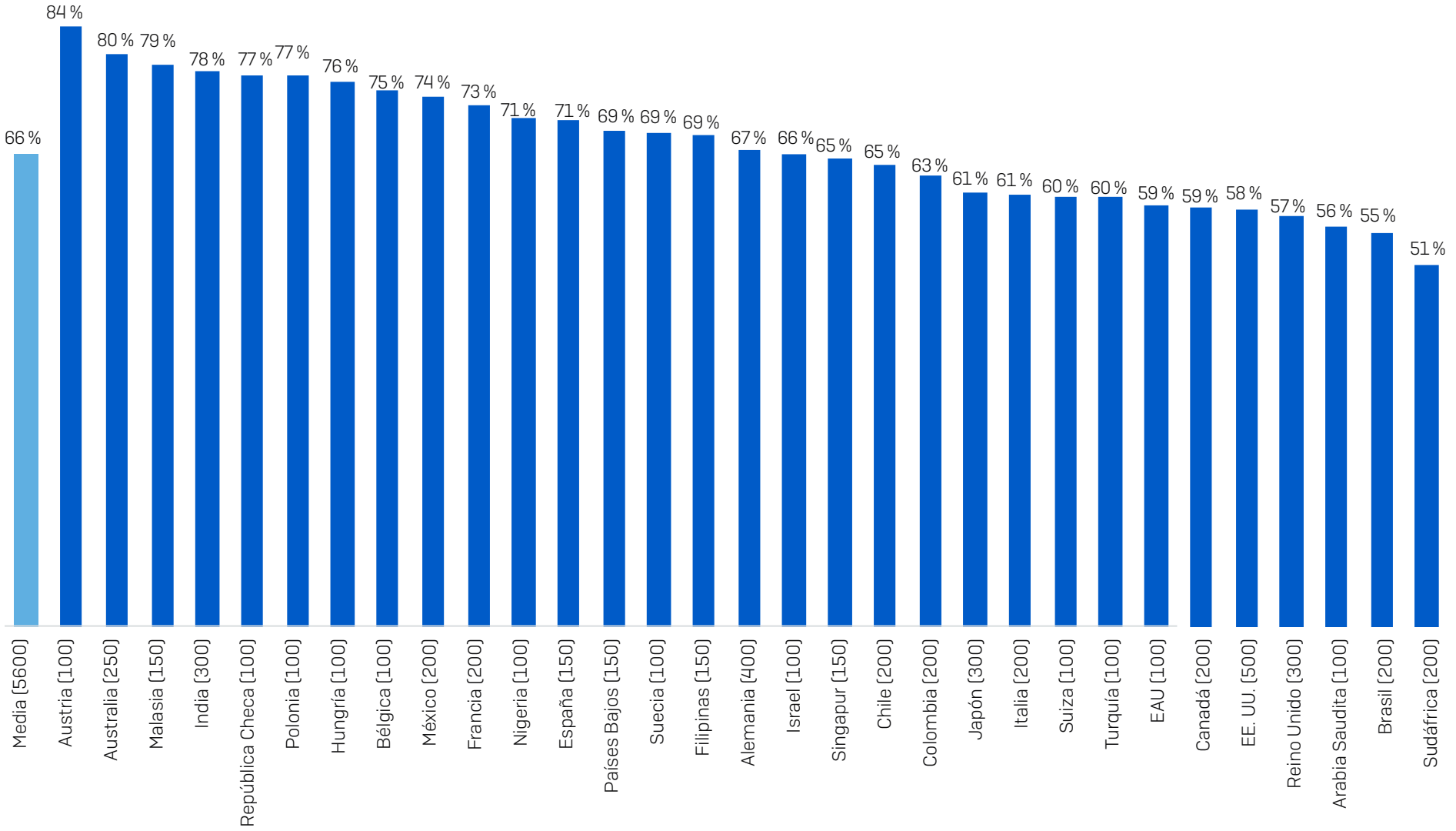
La mayoría de las organizaciones están optando por reducir el riesgo financiero asociado a un ataque contratando un ciberseguro. Para ellas, es tranquilizador saber que las aseguradoras pagan parte de los costes en casi todos los casos. Sin embargo, a las organizaciones les resulta cada vez más difícil obtener cobertura, lo que ha impulsado prácticamente a todas a introducir cambios en sus ciberdefensas para mejorar su posición frente a las aseguradoras.

Tanto si su objetivo es contar con la protección de un seguro o no, optimizar la ciberseguridad es imperativo para todas las organizaciones. Nuestros cinco consejos más importantes son:

- Garantice que las defensas en todos los puntos de su entorno sean de alta calidad. Revise los controles de seguridad y asegúrese de que siguen siendo válidos para sus necesidades.
- Busque las amenazas de forma proactiva con el fin de detener a los atacantes antes de que puedan ejecutar su ataque. Recurra a un especialista en MDR externo si no dispone del tiempo ni de los conocimientos necesarios.
- Refuerce su entorno buscando y cerrando las brechas de seguridad: dispositivos sin parchear, equipos sin proteger, puertos RDP abiertos, etc. La detección y respuesta ampliadas (XDR) es ideal en este sentido.
- Prepárese para lo peor. Sepa qué hacer en caso de un ciberincidente y con quién tiene que contactar.
- Haga copias de seguridad y practique la restauración de datos a partir de ellas. Su objetivo es recuperar su actividad lo más rápido posible con interrupciones mínimas.

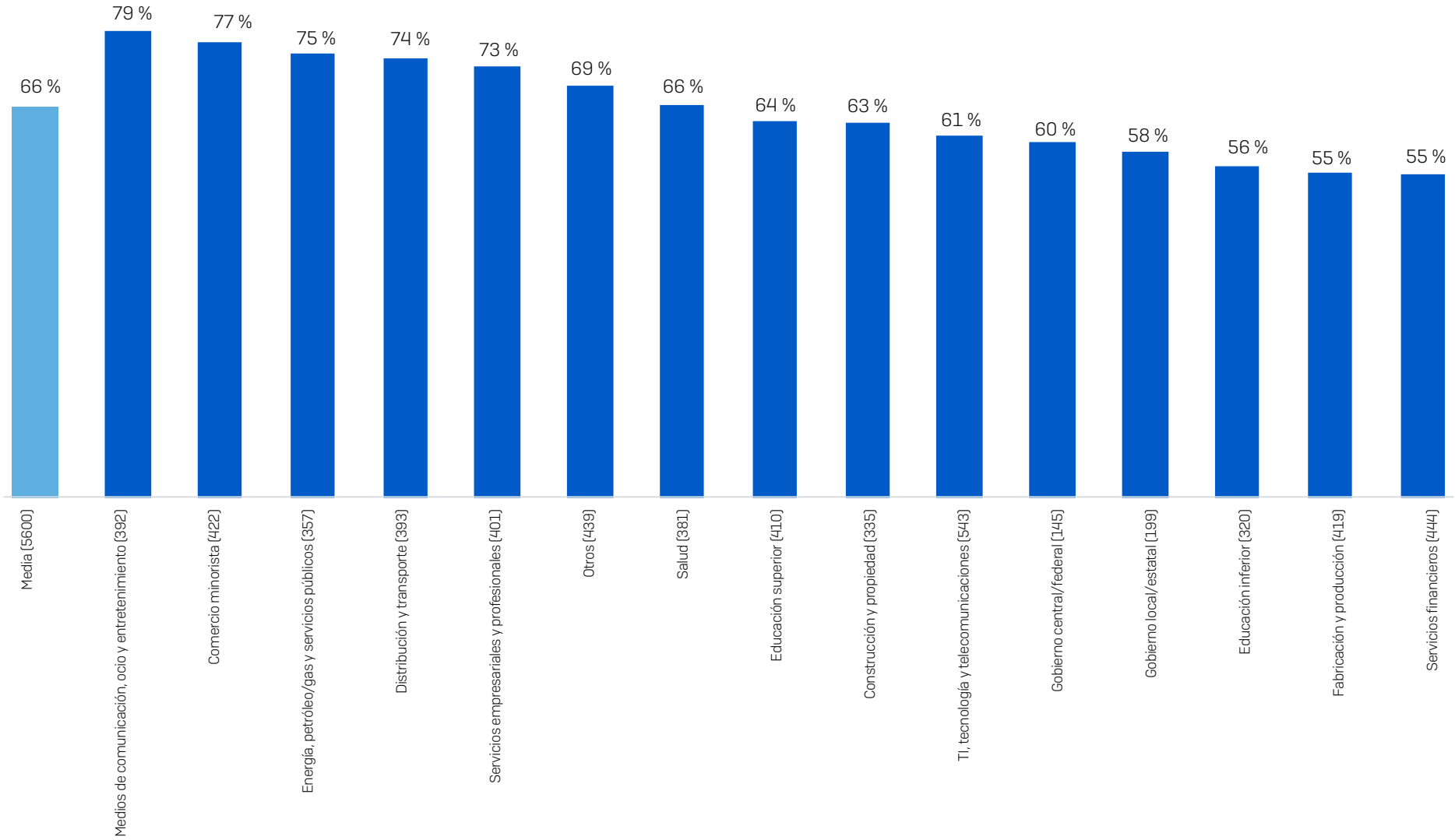
Consulte el Centro de información sobre amenazas de ransomware de Sophos para obtener información detallada sobre distintos grupos de ransomware.

Porcentaje de organizaciones afectadas por el ransomware en el último año



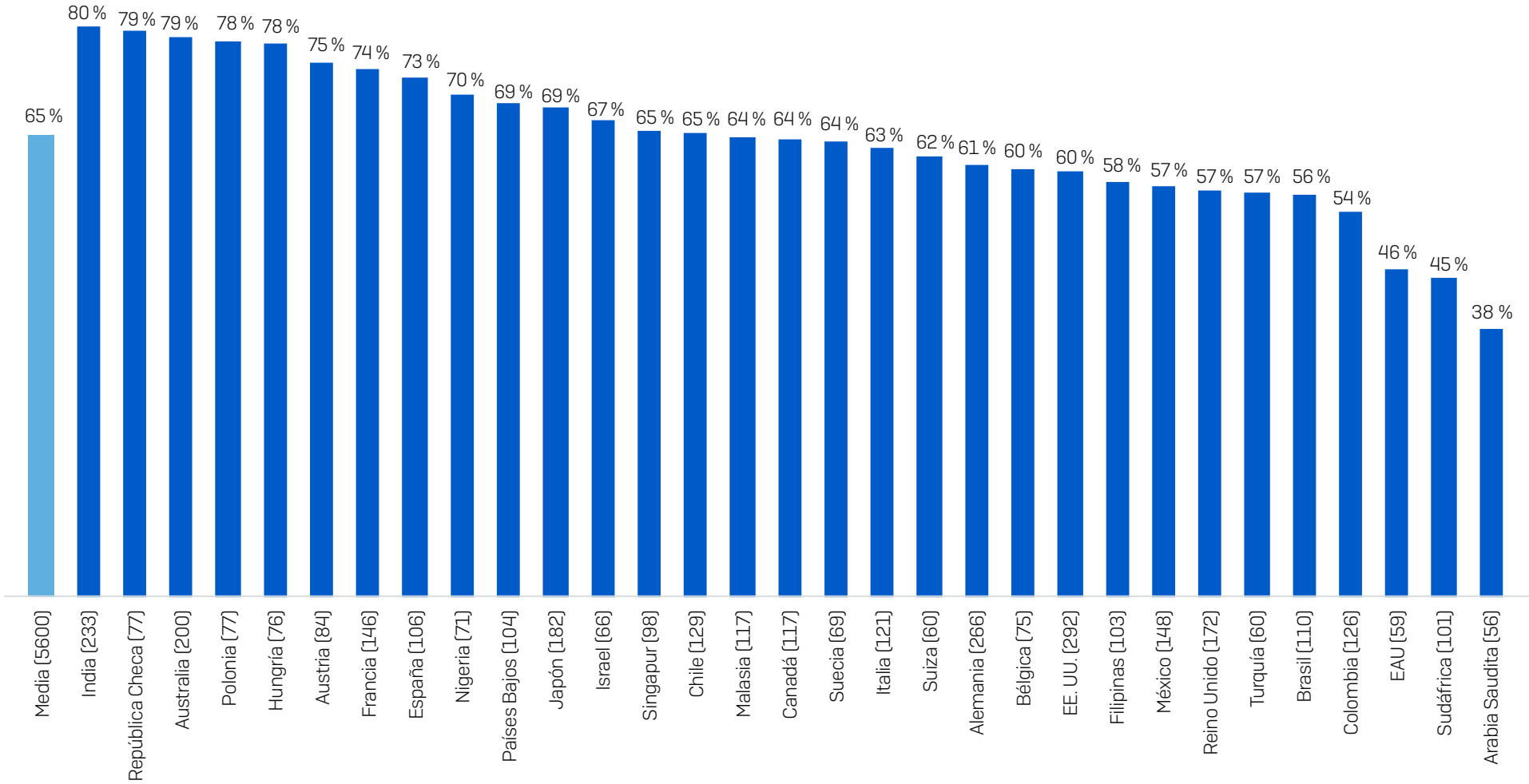
En el último año, ¿se ha visto afectada su empresa por el ransomware? (n=5600): Sí

Porcentaje de organizaciones afectadas por el ransomware en el último año



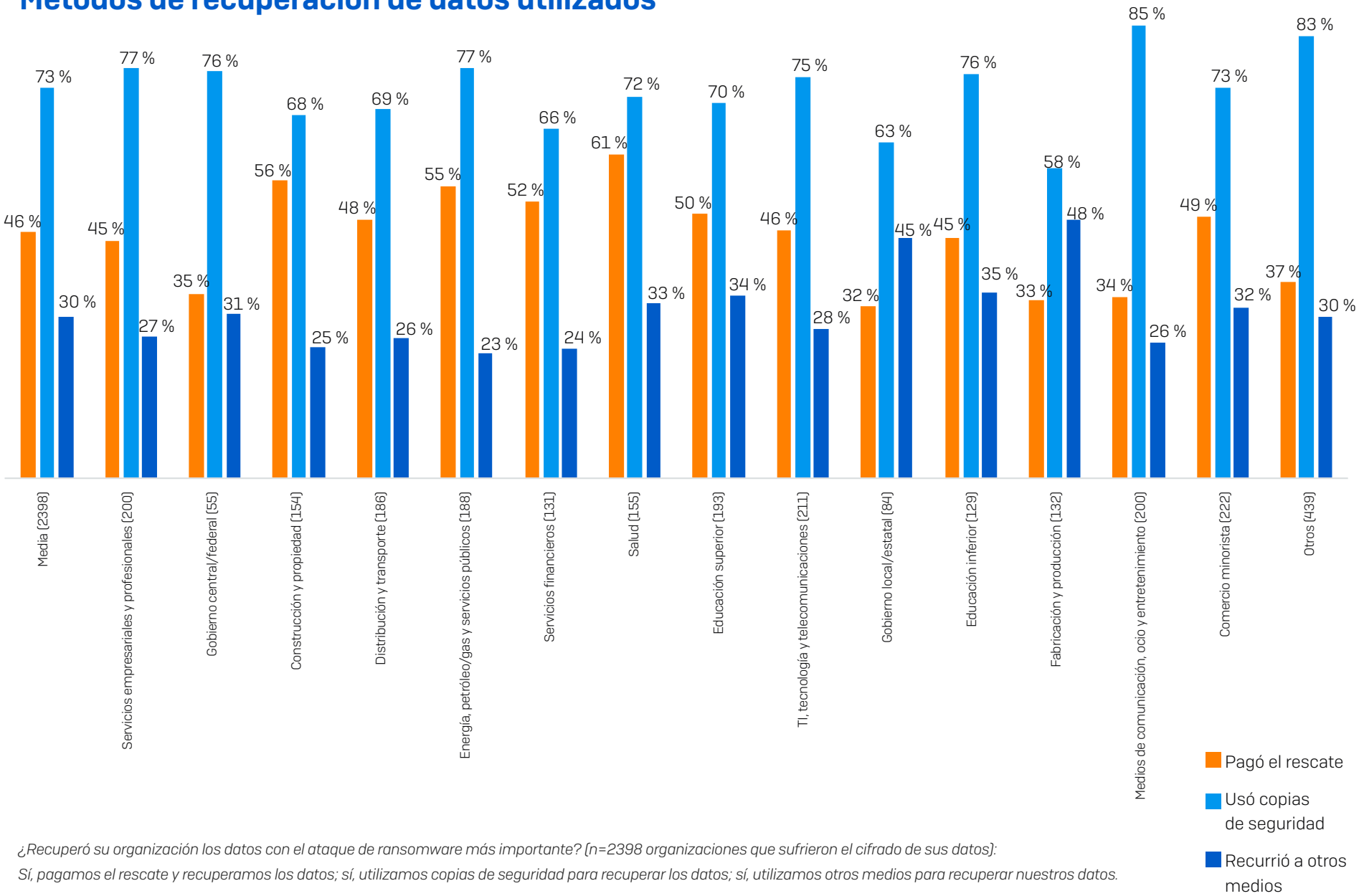
En el último año, ¿se ha visto afectada su empresa por el ransomware? (n=5600): Sí

Tasa de cifrado en ataques de ransomware



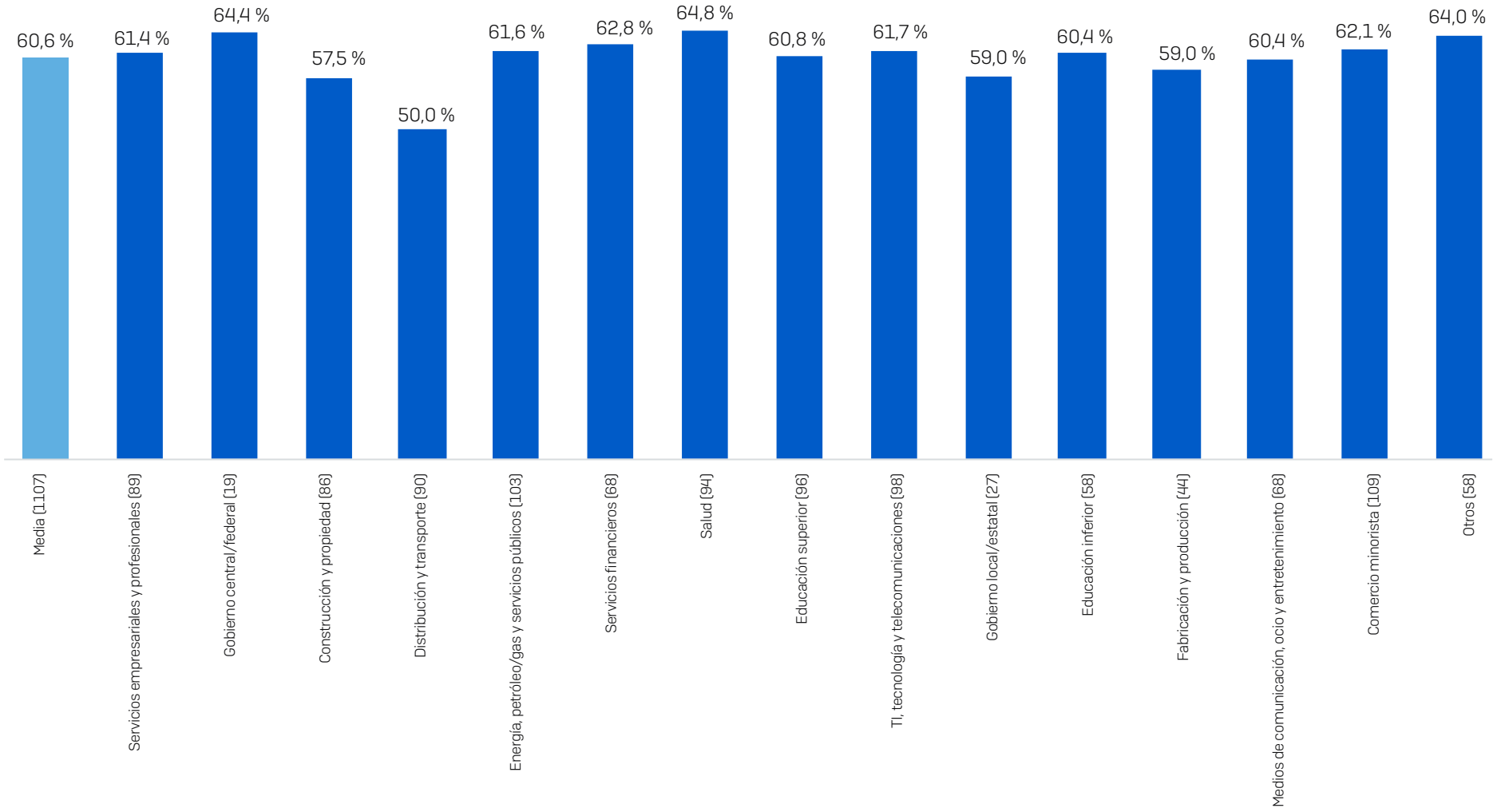
¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware más importante? (n=3702 organizaciones afectadas por el ransomware en el último año): Sí

Métodos de recuperación de datos utilizados



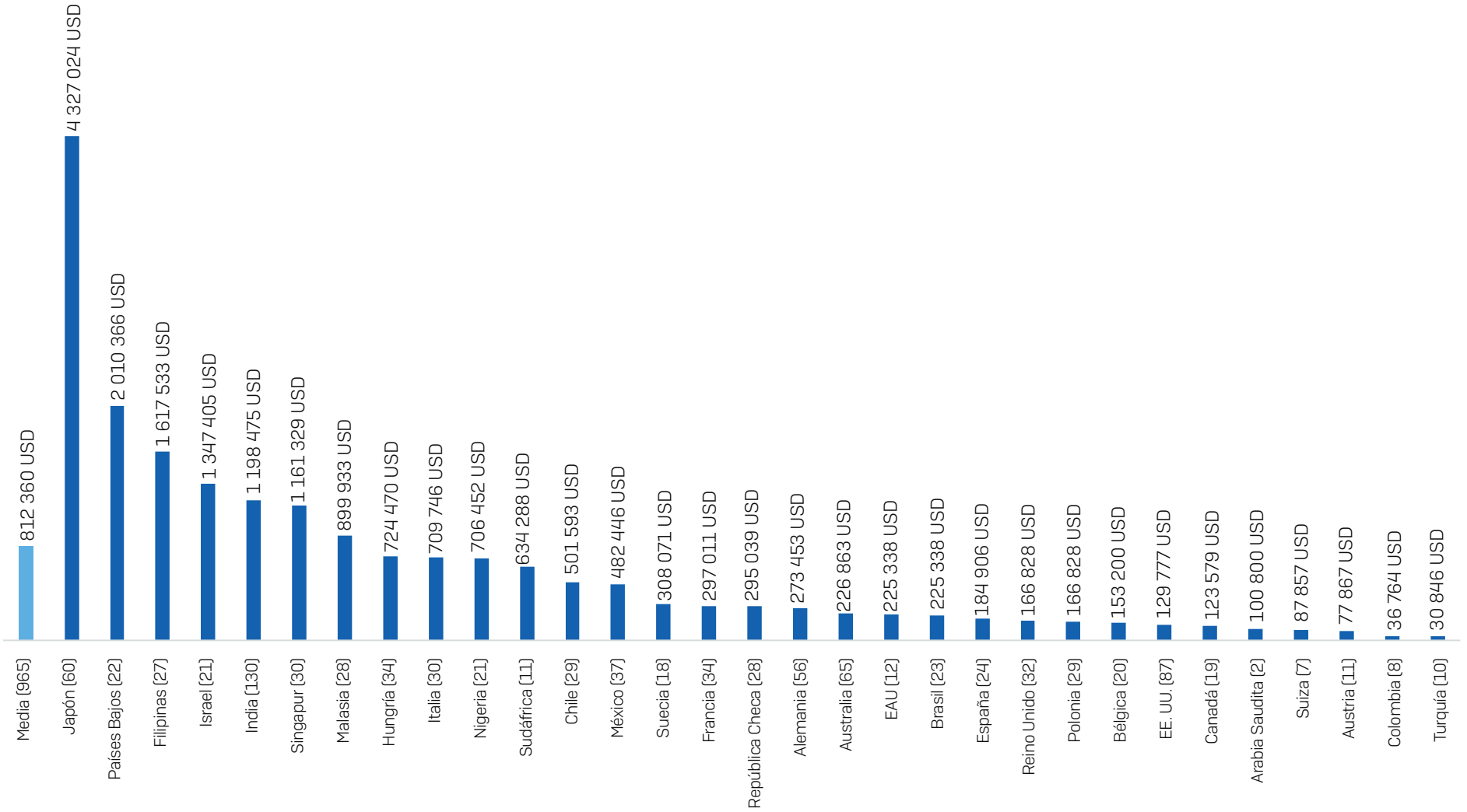
¿Recuperó su organización los datos con el ataque de ransomware más importante? (n=2398 organizaciones que sufrieron el cifrado de sus datos):
Sí, pagamos el rescate y recuperamos los datos; sí, utilizamos copias de seguridad para recuperar los datos; sí, utilizamos otros medios para recuperar nuestros datos.

Porcentaje de los datos restaurados después de pagar el rescate



¿Qué proporción de los datos recuperó su organización en el ataque de ransomware más importante?
(n=1107 organizaciones que pagaron el rescate y recuperaron los datos)

Media de pagos de rescate por país



¿Cuál fue el importe del rescate que pagó su organización en el ataque de ransomware más importante? USD. Número base en la tabla. Respuestas "No lo sé" y caso atípicos excluidos.
Nota: en el caso de los países con números base bajos, el resultado se debe considerar como meramente indicativo.

Coste medio de rectificación de un ataque (millones de USD)

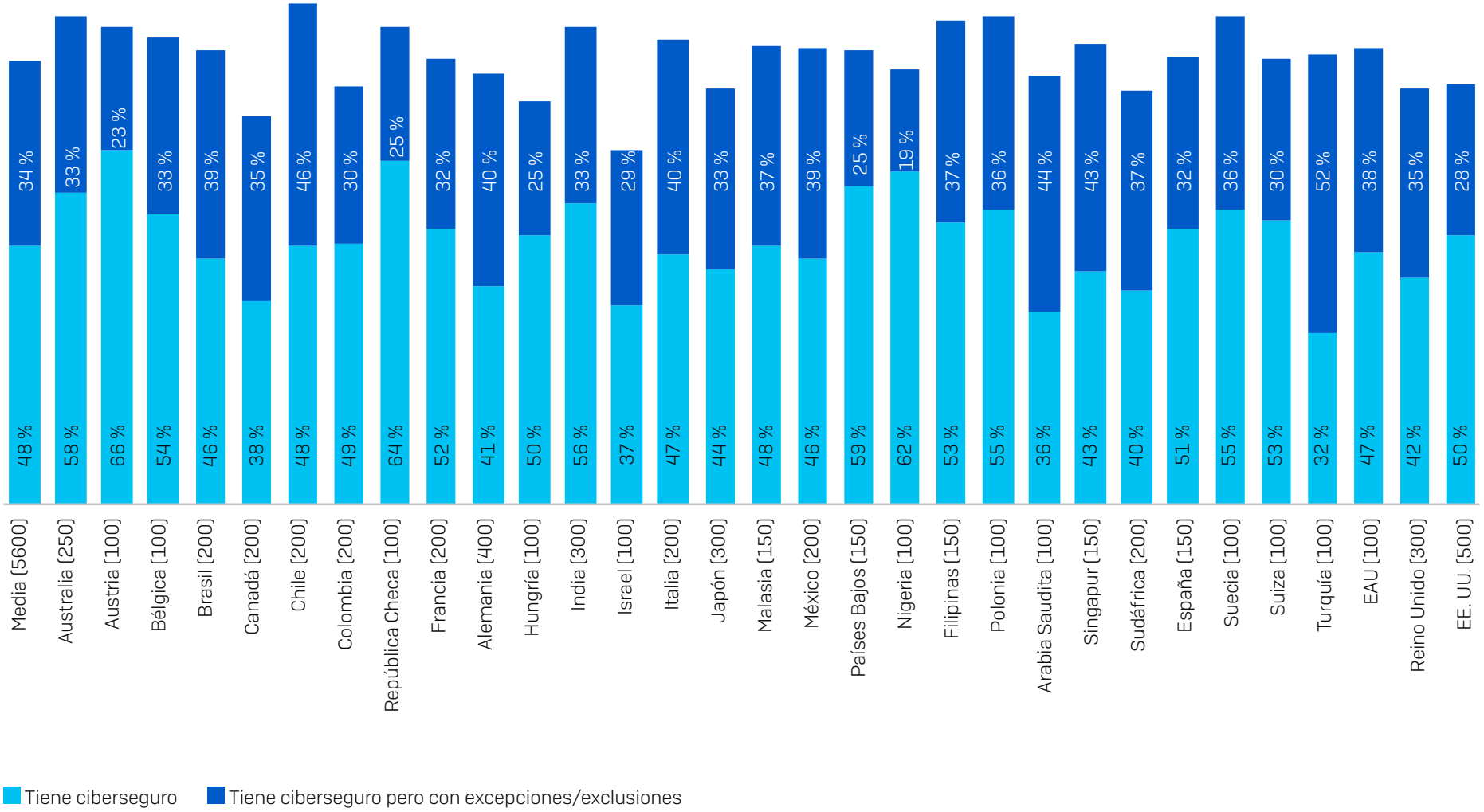
País	2021	2020	Variación anual
Media (3702)	1,40 USD	1,85 USD	-24 %
Australia (200)	1,01 USD	1,84 USD	-45 %
Austria (84)	0,81 USD	7,75 USD	-90 %
Bélgica (75)	3,71 USD	4,75 USD	-22 %
Brasil (110)	0,69 USD	0,82 USD	-16 %
Canadá (117)	0,65 USD	1,92 USD	-66 %
Chile (129)	1,58 USD	0,73 USD	116 %
Colombia (126)	0,50 USD	1,26 USD	-60 %
República Checa (77)	2,58 USD	0,37 USD	589 %
Francia (146)	2,03 USD	1,11 USD	83 %
Alemania (266)	1,73 USD	1,17 USD	48 %
Hungría (76)	1,51 USD	n/d	n/d
India (233)	2,81 USD	3,38 USD	-17 %
Israel (66)	1,41 USD	0,57 USD	148 %
Italia (121)	1,65 USD	0,68 USD	141 %
Japón (182)	0,96 USD	1,61 USD	-40 %
Malasia (118)	1,22 USD	0,77 USD	58 %

País	2021	2020	Variación anual
México (148)	0,88 USD	2,03 USD	-57 %
Países Bajos (104)	0,98 USD	2,71 USD	-64 %
Nigeria (71)	3,43 USD	0,46 USD	644 %
Filipinas (103)	1,34 USD	0,82 USD	63 %
Polonia (77)	1,78 USD	n/d	n/d
Arabia Saudita (56)	0,65 USD	0,21 USD	212 %
Singapur (98)	1,91 USD	3,46 USD	-45 %
Sudáfrica (101)	0,71 USD	n/d	n/d
España (106)	0,75 USD	0,60 USD	25 %
Suecia (69)	0,75 USD	1,40 USD	-46 %
Suiza (60)	1,64 USD	1,43 USD	15 %
Turquía (60)	0,37 USD	0,58 USD	-36 %
EAU (59)	1,26 USD	0,52 USD	144 %
Reino Unido (172)	1,08 USD	1,96 USD	-45 %
EE. UU. (292)	1,08 USD	2,09 USD	-49 %

Nota: números base solo para datos de 2021. *Nota: valores en millones de USD.*

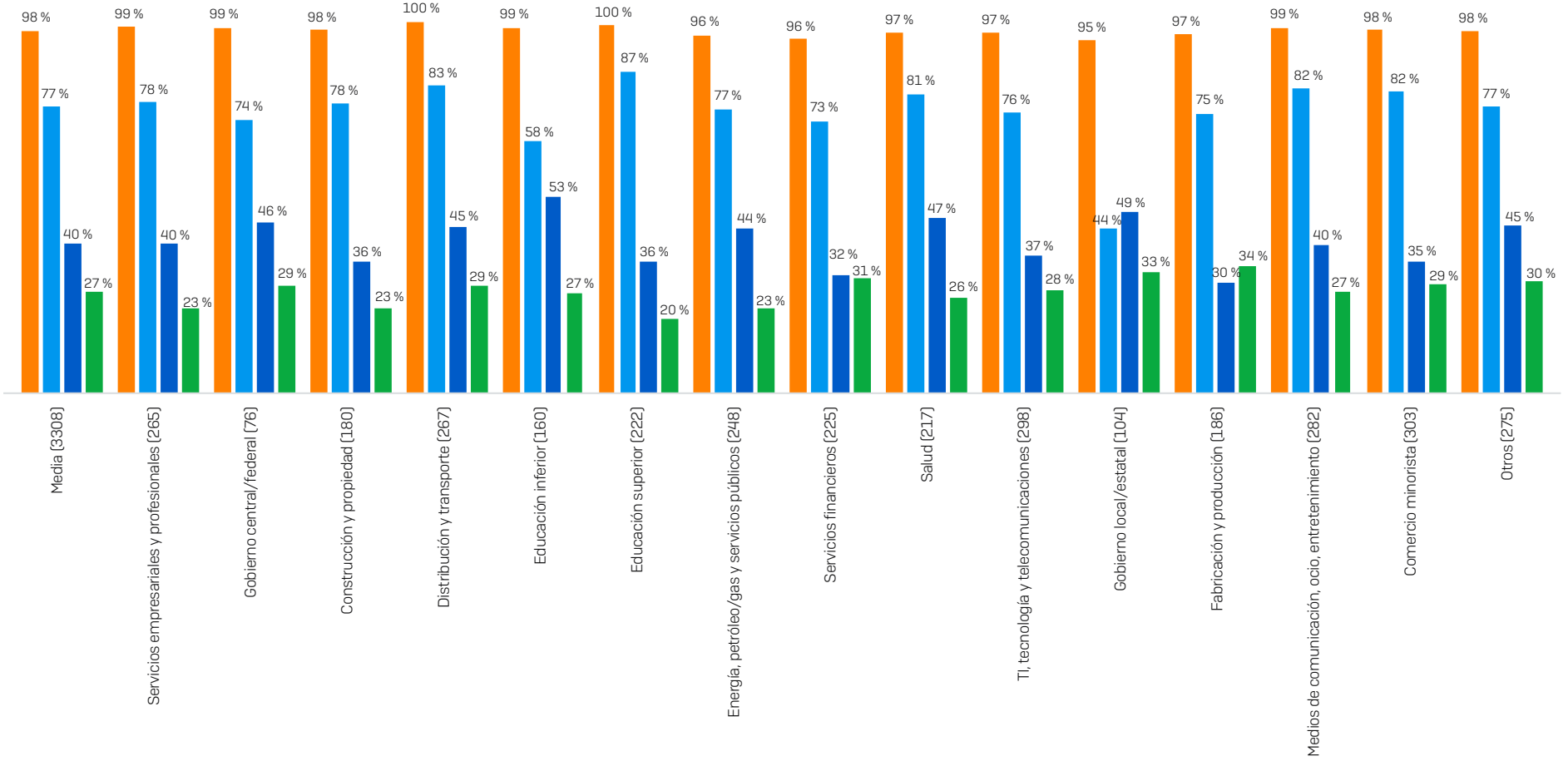
¿Cuál fue el coste aproximado para su empresa de rectificar los perjuicios del ataque de ransomware más reciente (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, el rescate pagado, etc.)? (n=3702 organizaciones afectadas por el ransomware en el año anterior)

Porcentaje de organizaciones con ciberseguro



¿Tiene su organización un ciberseguro que la cubra en caso de verse afectada por el ransomware? (n=5600). Sí; sí, pero con excepciones/exclusiones en nuestra póliza

Tasa de indemnización de los ciberseguros



¿Le indemnizó el ciberseguro por los costes asociados al ataque de ransomware más importante sufrido por su organización? (n=3308 organizaciones que se vieron afectadas por el ransomware en el año anterior y que contaban con un ciberseguro para ransomware). Sí, pagó los costes de limpieza (es decir, los costes para recuperar la actividad); sí, pagó el rescate; sí, pagó otros gastos (p. ej., tiempo de inactividad, pérdidas de oportunidad de negocio, etc.)

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

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 empresa estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

04-04-2022 (WP-NP)

SOPHOS