SOPHOS
Cybersecurity delivered.

El estado del ransomware en el sector minorista 2022

Resultados de una encuesta independiente y desvinculada de cualquier proveedor a 5600 profesionales de TI de organizaciones de tamaño medio en 31 países, incluidos 422 responsables del sector minorista.

Monográficos de Sophos. Septiembre de 2022

Introducción

El estudio anual de Sophos sobre las experiencias reales con ransomware de los profesionales de TI en el sector minorista ha revelado la existencia de un entorno hostil cada vez más desafiante, además de la creciente carga tanto operativa como financiera a la que el ransomware somete a sus víctimas. También arroja nueva luz sobre la relación entre el ransomware y los ciberseguros, incluyendo 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, incluidos 422 del sector minorista. Los encuestados pertenecían a organizaciones medianas (100 a 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.

5600
encuestados

422
Encuestados minoristas

31
países

100-5000
empleados

Ene/feb 2022
fecha de encuesta

Los ataques de ransomware aumentan respecto al año pasado

El 77 % de las organizaciones minoristas se vieron afectadas por el ransomware en 2021, frente al 44 % en 2020. Esto representa una subida del 75 % en el transcurso de un año, lo que demuestra que los adversarios se han vuelto considerablemente más capaces de ejecutar ataques a escala. De hecho, en 2021, el sector minorista registró la segunda cifra más alta de ataques de ransomware de todos los sectores analizados. A modo de comparación, el 66 % de los encuestados de todos los sectores afirmaron haber sufrido un ataque de ransomware en el último año. [Nota: por organización afectada por el ransomware se entiende uno o más dispositivos afectados, pero sin implicar necesariamente su cifrado.]

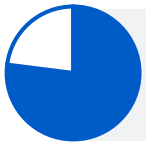
El sector minorista registró un índice superior a la media no solo de ataques de ransomware, sino también de cifrado de datos: un 68 % de las víctimas lo sufrieron frente a un 65 % de media en todos los sectores. Tan solo el 28 % de encuestados del sector dijeron que lograron detener el ataque antes de que se pudieran cifrar los datos, lo que está por debajo de la media de todos los sectores del 31 %.

Curiosamente, en el sector minorista se observó un notable descenso en los ataques de solo extorsión, del 12 % en 2020 al 3 % en 2021. Aunque aparentemente esto es bueno, en Sophos hemos visto un incremento en el número de adversarios que combinan tanto el ransomware como la extorsión con el fin de mejorar la efectividad de sus campañas. Por tanto, es probable que esta caída refleje un cambio en las tácticas de los adversarios más que un alejamiento de la extorsión con datos.

El aumento de los ataques de ransomware que logran su objetivo forma parte de un entorno de amenazas cada vez más desafiante que ha afectado a organizaciones de todos los sectores, incluido el minorista.

En el último año, el 55 % de los encuestados de este sector indicaron que había aumentado el volumen de los ataques, el 55 % vieron aumentar la complejidad de los ataques, y el 51 % afirmaron que había aumentado su impacto en su organización. Si bien son preocupantes estas cifras, están por debajo de la media de todos los sectores, lo que indica que el sector minorista se ve menos afectado que otros.

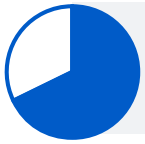
Afectados por el ransomware



77 %
Organizaciones minoristas
(el segundo más alto de todos los sectores)

66 %
Media de todos los sectores

Datos cifrados en el ataque



68 %
Organizaciones minoristas

65 %
Media de todos los sectores

Aumento del volumen, la complejidad y el impacto de los ataques en el último año

	AUMENTO DEL VOLUMEN DE LOS CIBERATAQUES	AUMENTO DE LA COMPLEJIDAD DE LOS CIBERATAQUES	AUMENTO DEL IMPACTO DE LOS CIBERATAQUES
Sector minorista	55 %	55 %	51 %
Media de todos los sectores	57 %	59 %	53 %

La mayoría de las víctimas del sector minorista recuperó algunos datos cifrados

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 minoristas (99 %) afectadas por el ransomware durante el último año y cuyos datos fueron cifrados lograron recuperar parte de los datos cifrados.

Las copias de seguridad fueron el principal método utilizado para restaurar los datos cifrados. Casi tres de cada cuatro (73 %) organizaciones minoristas cuyos datos fueron cifrados utilizaron este método en 2021, un aumento considerable con respecto al 56 % en 2020.

A pesar del uso generalizado de las copias de seguridad, el 49 % de los encuestados del sector afirmaron haber pagado el rescate para recuperar sus datos. Este índice de pago de rescate está por encima de la media de todos los sectores, que fue del 46 % en 2021, y constituye un importante aumento con respecto al 32 % de los encuestados del sector minorista que afirmaron haber pagado el rescate en 2020. Además, casi un tercio (32 %) afirmó usar otros medios para restaurar sus datos.

Los porcentajes de uso de copias de seguridad, pago del rescate y uso de otros métodos suman mucho más del 100 %, lo que indica que muchas organizaciones minoristas utilizan varias estrategias de restauración en paralelo. En general, el 46 % de las víctimas del sector minorista utilizaron varios métodos para restaurar sus datos.

Método de restauración de datos

	PAGARON EL RESCATE	USARON COPIAS DE SEGURIDAD	USARON OTROS MEDIOS	MÚLTIPLES MÉTODOS USADOS
Sector minorista	49 %	73 %	32 %	46 %
Media de todos los sectores	46 %	73 %	30 %	44 %

Recuperación de parte de los datos cifrados

Se recuperan menos datos tras pagar el rescate

La cantidad media de datos recuperados en todos los sectores tras pagar el rescate sufrió un descenso en el último año, del 65 % en 2020 al 61 % en 2021. El sector minorista vio una tendencia a la baja similar, ya que recuperó una media del 62 % de los datos en 2021 frente al 67 % registrado en 2020.

Al mismo tiempo, el porcentaje de organizaciones minoristas que recuperaron TODOS sus datos también disminuyó: solo el 5 % restauraron todos sus datos cifrados en 2021 frente al 9 % en 2020.

La conclusión principal es que, pagando el rescate, solamente se recupera parte de los datos cifrados y que no se puede contar con el pago del rescate para recuperar todos los datos.

Porcentaje de datos restaurados después de pagar el rescate

62 %
Sector minorista

61 %
Media de todos los sectores

Porcentaje que recuperó TODOS sus datos después de pagar el rescate

5 %
Sector minorista

4 %
Media de todos los sectores

El importe de rescate en el sector minorista es bajo

965 encuestados de organizaciones de todos los sectores que pagaron el rescate revelaron la cifra exacta, lo que ha permitido constatar que el importe medio de los pagos de rescate aumentó de forma importante 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).

88 encuestados del sector minorista compartieron el importe exacto que pagaron, y el rescate medio resultó ser de 226 044 USD.

Aunque es alentador que este año el pago de rescate medio en el sector minorista no llega a un tercio de la media de todos los sectores, representa un aumento considerable con respecto a los 147 811 USD indicados en 2020 por 36 encuestados del sector. Es evidente que el sector minorista no ha podido escapar a la tendencia global al alza en los pagos de los rescates en el último año.

Si profundizamos en los importes de estos rescates, vemos que más de una quinta parte (22 %) de las organizaciones minoristas pagaron menos de 1000 USD, mientras que dos tercios (70 %) pagaron un importe inferior a los 100 000 USD. Estos pagos bajos ayudan a mantener a raya la media del sector en comparación con muchas otras industrias.

Asimismo, solo el 29 % de los encuestados del sector minorista pagaron 100 000 USD o más frente al 47 % de todos los encuestados a escala global. Solo el 4 % de las organizaciones minoristas pagaron 1 millón USD o más, lo que está muy por debajo de la media de todos los sectores del 11 %.

Rescate pagado por las organizaciones minoristas

226 000 USD Sector minorista

812 000 USD Media de todos los sectores

22 %
Pagaron menos de 1000 USD

70 %
Pagaron menos de 100 000 USD

29 %
Pagaron 100 000 USD o más

4 %
Pagaron 1 millón USD o más

El ransomware tiene un importante impacto financiero, comercial y operativo en el sector minorista

Las sumas de los rescates son solo una parte de la historia, y el impacto del ransomware abarca mucho más que el cifrado de bases de datos y dispositivos.

El 92 % de las organizaciones minoristas afectadas por el ransomware afirmaron que el ataque afectó a su capacidad operativa (media de todos los sectores: 90 %), mientras que el 89 % dijeron que el ataque causó pérdidas de negocio/ingresos a su organización (media de todos los sectores: 86 %). Estos puntos de datos indican que el impacto operativo y comercial del ransomware en el sector minorista fue un poco superior a la media de todos los sectores.

Con respecto a la factura general de remediación de costes, el coste medio en todos los sectores para que una organización subsanara el impacto del ataque de ransomware más reciente fue de 1,4 millones USD en 2021, por debajo de los 1,85 millones USD de 2020.

Siguiendo esta misma línea, el coste general para las organizaciones minoristas de remediar un ataque de ransomware también cayó de 1,97 millones USD en 2020 a 1,27 millones USD en 2021.

Existen varios factores que probablemente contribuyen a este coste inferior a la media para el sector minorista. El primero es un índice más elevado de cobertura de ciberseguridad en este sector, cuestión que abordaremos más adelante en este informe. Las aseguradoras suelen estar 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. En segundo lugar, es probable que el aumento inferior a la media de la complejidad y el impacto de los ataques de ransomware en el sector minorista haya tenido una repercusión acorde en los costes de recuperación.

En lo que respecta al tiempo invertido en recuperarse de un ataque de ransomware, el sector minorista siguió la media de todos los sectores: un poco más de la mitad (53 %) de las organizaciones minoristas se recuperaron en un plazo de una semana. Menos de uno de cada cinco (17 %) encuestados del sector afirmaron que tardaron entre uno y seis meses en recuperarse.

Impacto en la capacidad operativa

92 %
Sector minorista

90 %
Media de todos los sectores

Impacto en el negocio/ingresos

89 %
Sector minorista

86 %
Media de todos los sectores

Coste medio de remediación del ataque más reciente

1,27 millones USD Sector minorista

1,40 millones USD Media de todos los sectores

Tiempo de recuperación tras ataques de ransomware

DURACIÓN	SECTOR MINORISTA	MEDIA DE TODOS LOS SECTORES
Hasta una semana	53 %	53 %
En 1-6 meses	17 %	20 %

El sector minorista tiene el segundo índice más alto en cobertura de ciberseguridad contra el ransomware

El 88 % de los encuestados minoristas afirmaron que tenían cobertura contra los ataques de ransomware, frente a una media del 83 % en todos los sectores.

Para el 93 % de las organizaciones minoristas con un ciberseguro, el proceso de obtención de la cobertura ha cambiado en el último año:

- Según el 41 %, el número de aseguradoras que ofrecen ciberseguros ha bajado.
- Según el 57 %, el nivel de ciberseguridad necesario para optar a un ciberseguro ha aumentado.
- Según el 43 %, las pólizas ahora son más complejas.
- Según el 37 %, el proceso es más largo.
- Según el 35 %, es más caro.

Estos cambios están estrechamente relacionados con el ransomware, que es el principal motivo de las reclamaciones de ciberseguros. En los últimos años, los ataques de ransomware han aumentado y los rescates y costes de pago se han disparado. Como resultado, algunas aseguradoras han abandonado el mercado, ya que simplemente no les resultaba rentable.

Al haber menos organizaciones que ofrecen cobertura de ciberseguridad, es un mercado dominado por los vendedores. Son ellos los que mandan y pueden ser selectivos con los clientes a los que ofrecen cobertura. Las aseguradoras que quedan buscan reducir el riesgo y la exposición, y también están subiendo los precios de forma importante. Contar con unas ciberdefensas sólidas mejorará significativamente la capacidad una organización para conseguir la cobertura que necesita.

Los ciberseguros empujan al sector minorista a mejorar las ciberdefensas

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 minoristas con un ciberseguro han introducido cambios en su ciberdefensa para mejorar su posición frente a las aseguradoras:

- El 66 % ha implementado nuevos servicios/tecnologías.
- El 55 % ha aumentado las actividades de formación/educación del personal.
- El 53 % ha cambiado procesos/conductas.

Los ciberseguros propician la mejora de las ciberdefensas

	HAN CAMBIADO SUS CIBERDEFENSAS PARA MEJORAR SU POSICIÓN FRENTE A LAS ASEGURADORAS	HAN IMPLEMENTADO NUEVOS SERVICIOS/ TECNOLOGÍAS	HAN AUMENTADO LAS ACTIVIDADES DE FORMACIÓN/ CONCIENCIACIÓN DEL PERSONAL	HAN CAMBIADO PROCESOS/ CONDUCTAS
Sector minorista	97 %	66 %	55 %	53 %
Media de todos los sectores	97 %	64 %	56 %	52 %

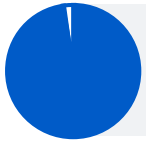
El sector minorista tiene una tasa de indemnización de rescates inferior a la media

En todos los sectores, los ciberseguros casi siempre pagan parte de los costes en caso de un ataque de ransomware. Las organizaciones minoristas con ciberseguros contra el ransomware registraron una tasa de indemnización del 98 %, que está en la línea de la media de todos los sectores.

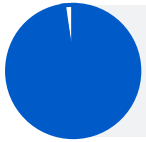
Según el sector minorista, los seguros pagaron los costes de limpieza en el 82 % de los ataques, una cifra superior a la media del 77 % de todos los sectores. Sin embargo, cabe destacar que los encuestados minoristas registraron una tasa de indemnización de rescates inferior a la media: la aseguradora pagó el rescate en el 35 % de los ataques frente al 40 % de media en todos los sectores. Esto sugiere que, a menudo, las víctimas pagan los rescates de sus propios bolsillos.

Vale la pena 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.

Tasa de indemnización de los ciberseguros:

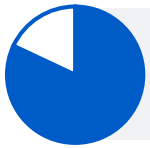


98 %
Sector minorista



98 %
Media de todos los sectores

Pago de los costes de limpieza:



82 %
Sector minorista

77 %
Media de todos los sectores

Pago del rescate:

35 %
Sector minorista

40 %
Media de todos los sectores

Conclusión

El desafío que el ransomware representa para las organizaciones minoristas no deja de crecer. La proporción de organizaciones afectadas por el ransomware ha aumentado considerablemente en doce meses, puesto que los ciberdelincuentes han logrado cifrar los datos en más de la mitad de los ataques.

En vista de esta casi normalización del ransomware, las organizaciones minoristas han mejorado en lo que respecta a solventar las secuelas de un ataque: ahora, prácticamente todas (99 %) recuperan parte de los datos cifrados. Las copias de seguridad fueron el principal método utilizado para restaurar los datos cifrados.

El índice de pago de rescates de las organizaciones minoristas es superior a la media, con un 49 % frente a la media de todos los sectores del 46 %. A su vez, el rescate medio pagado en este sector fue de menos de un tercio de la media de todos los sectores. La proporción de datos cifrados recuperados por las organizaciones minoristas tras pagar el rescate es algo superior a la media: un 62 % frente a un 61 %.

El coste general de remediar un ataque de ransomware en el sector minorista cayó en el último año (de 1,97 millones USD en 2020 a 1,27 millones USD en 2021) y sigue por debajo de la media de todos los sectores, que este año ascendió a 1,4 millones USD.

Muchas organizaciones minoristas optan por reducir el riesgo asociado a los ataques de ransomware contratando un ciberseguro. Para ellas, es tranquilizador saber que las aseguradoras pagan parte de los costes en casi todos los casos. Sin embargo, aunque el sector minorista tiene una tasa de indemnización de costes de limpieza superior a la media, no pasa lo mismo con su tasa de indemnización de rescates, que se sitúa por debajo.

Las organizaciones minoristas cada vez lo tienen más difícil para conseguir la cobertura de un ciberseguro. Esto ha llevado prácticamente a todas ellas a introducir cambios en sus ciberdefensas para mejorar su posición frente a las aseguradoras.

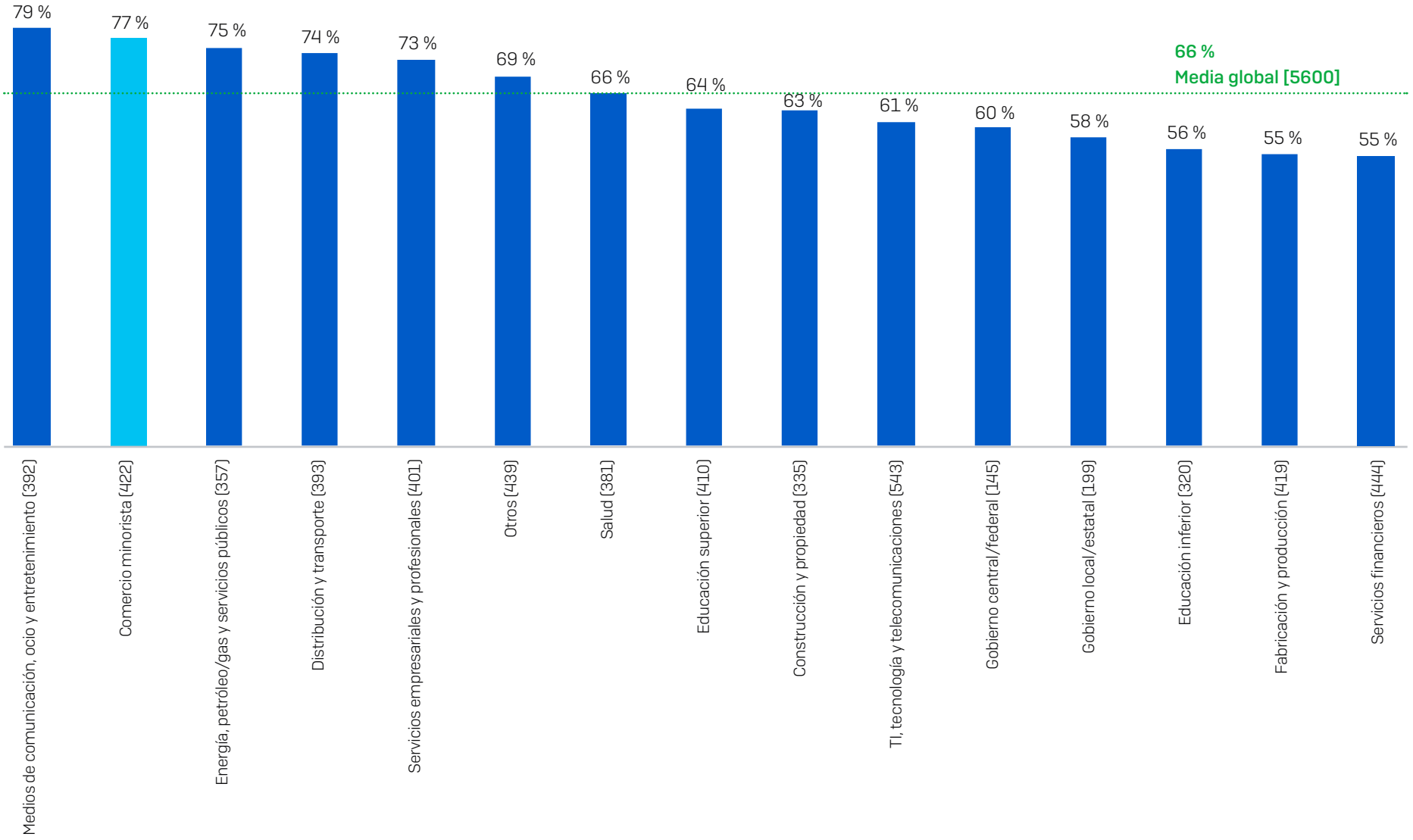
Recomendaciones

En vista de estos resultados, optimizar las defensas contra el ransomware es más importante que nunca. 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. Trabaje con un servicio especializado en ciberseguridad MDR (detección y respuesta gestionadas) si no dispone del tiempo ni de los conocimientos necesarios a nivel interno.
- 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.

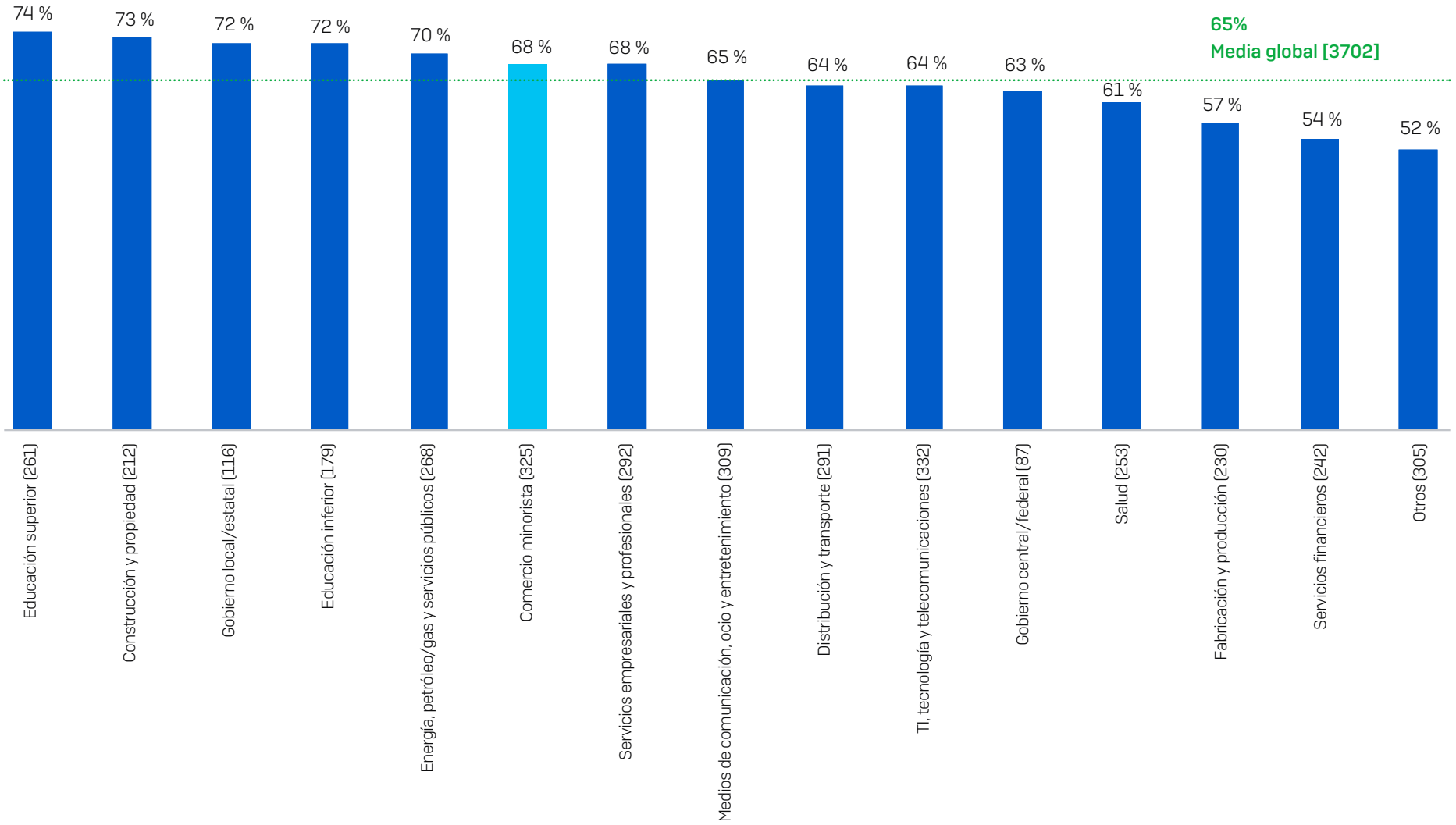
Consulte el Centro de información sobre amenazas de ransomware de Sophos para obtener información detallada sobre distintos grupos de ransomware.

El sector minorista registra uno de los índices más altos de ataques de ransomware



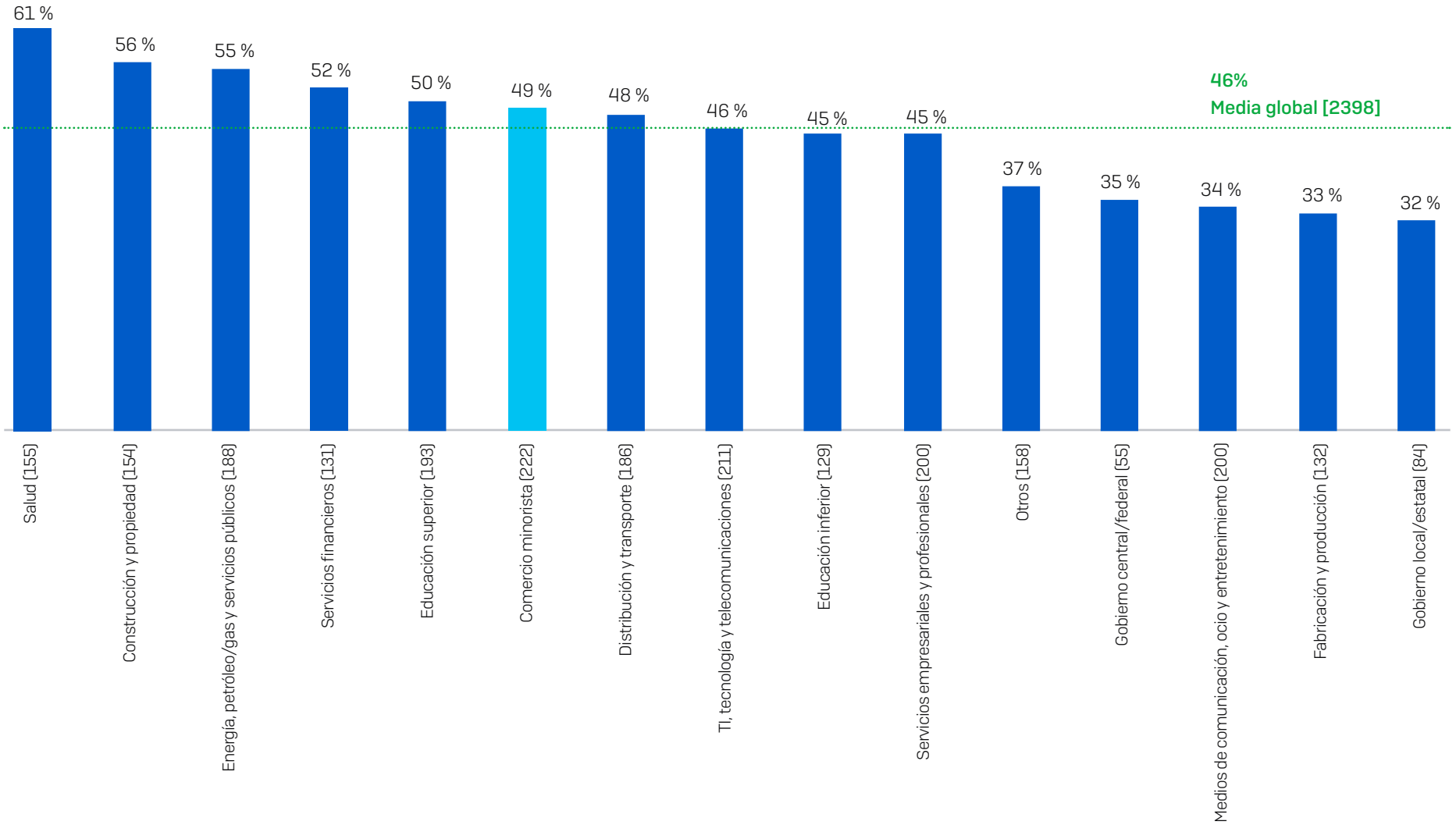
En el último año, ¿se ha visto afectada su organización por el ransomware? (n=5600): Sí

El sector minorista tiene un índice de cifrado superior a la media



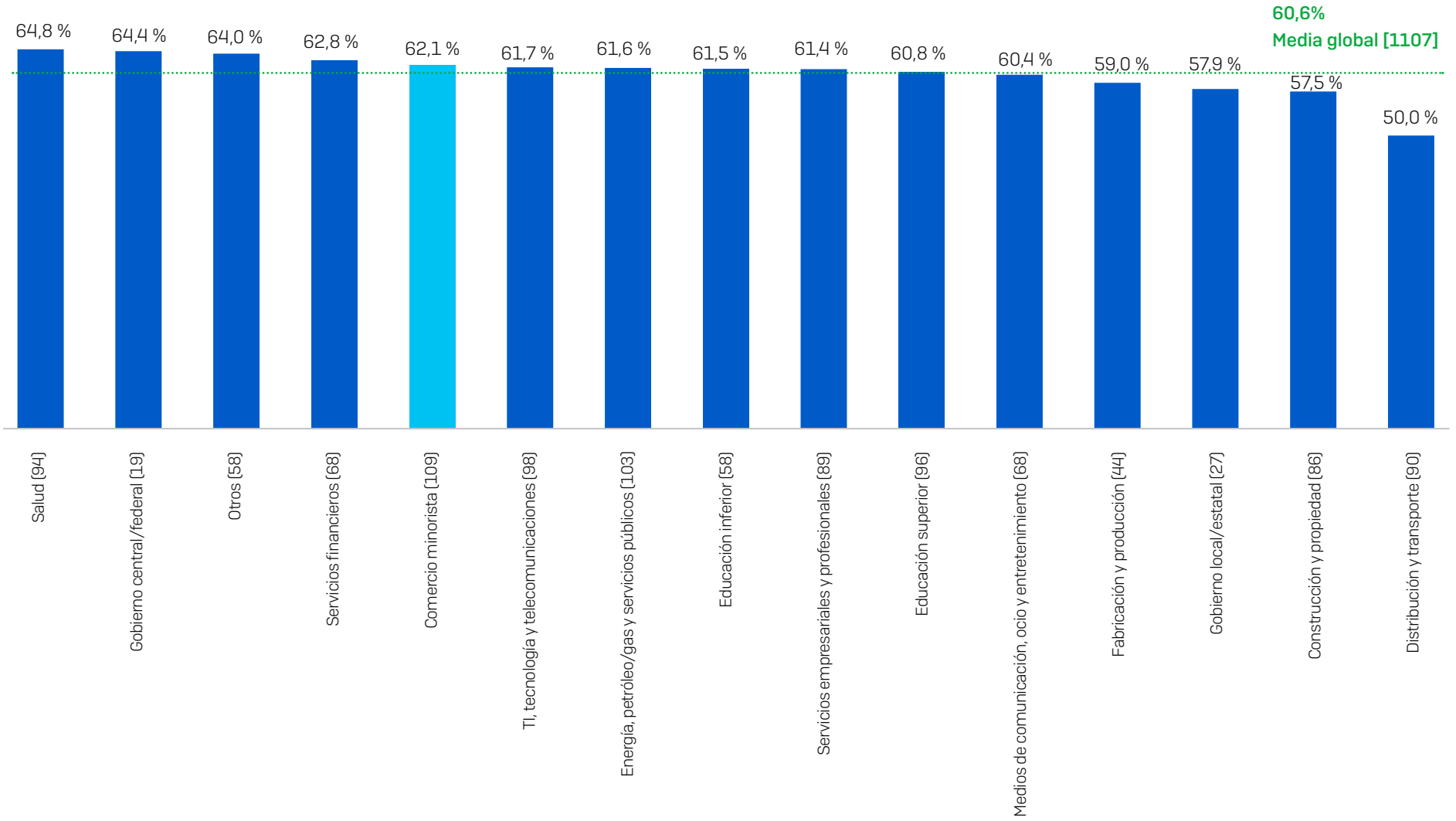
¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware más importante?
(n=3702 organizaciones afectadas por el ransomware en el último año): Sí

El sector minorista tiene un índice de pago de rescates superior a la media



¿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

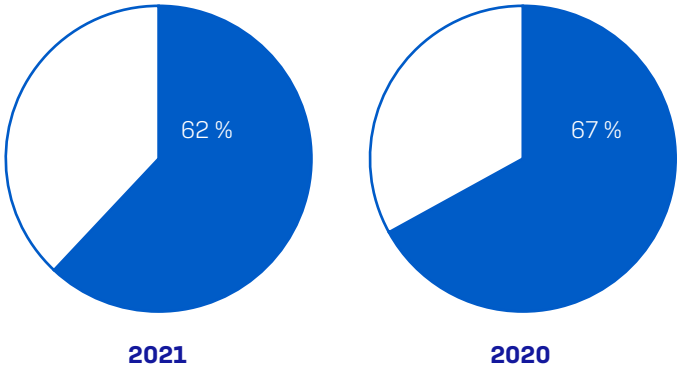
El sector minorista recupera más datos que la media tras pagar el rescate



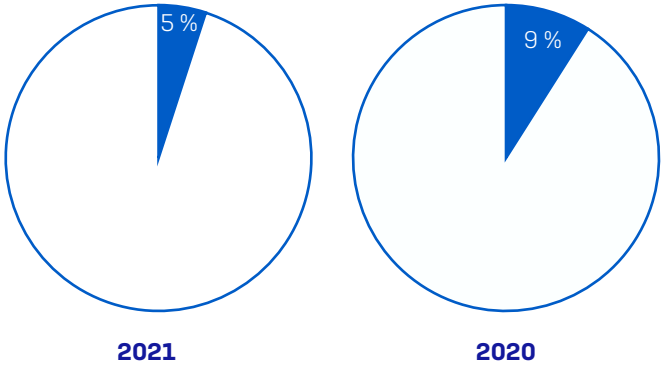
¿Qué proporción de los datos recuperó su organización en el ataque de ransomware más importante?
(1107 organizaciones que pagaron el rescate y recuperaron datos)

Las organizaciones minoristas recuperaron menos datos en el último año

Porcentaje de datos restaurados después de pagar el rescate

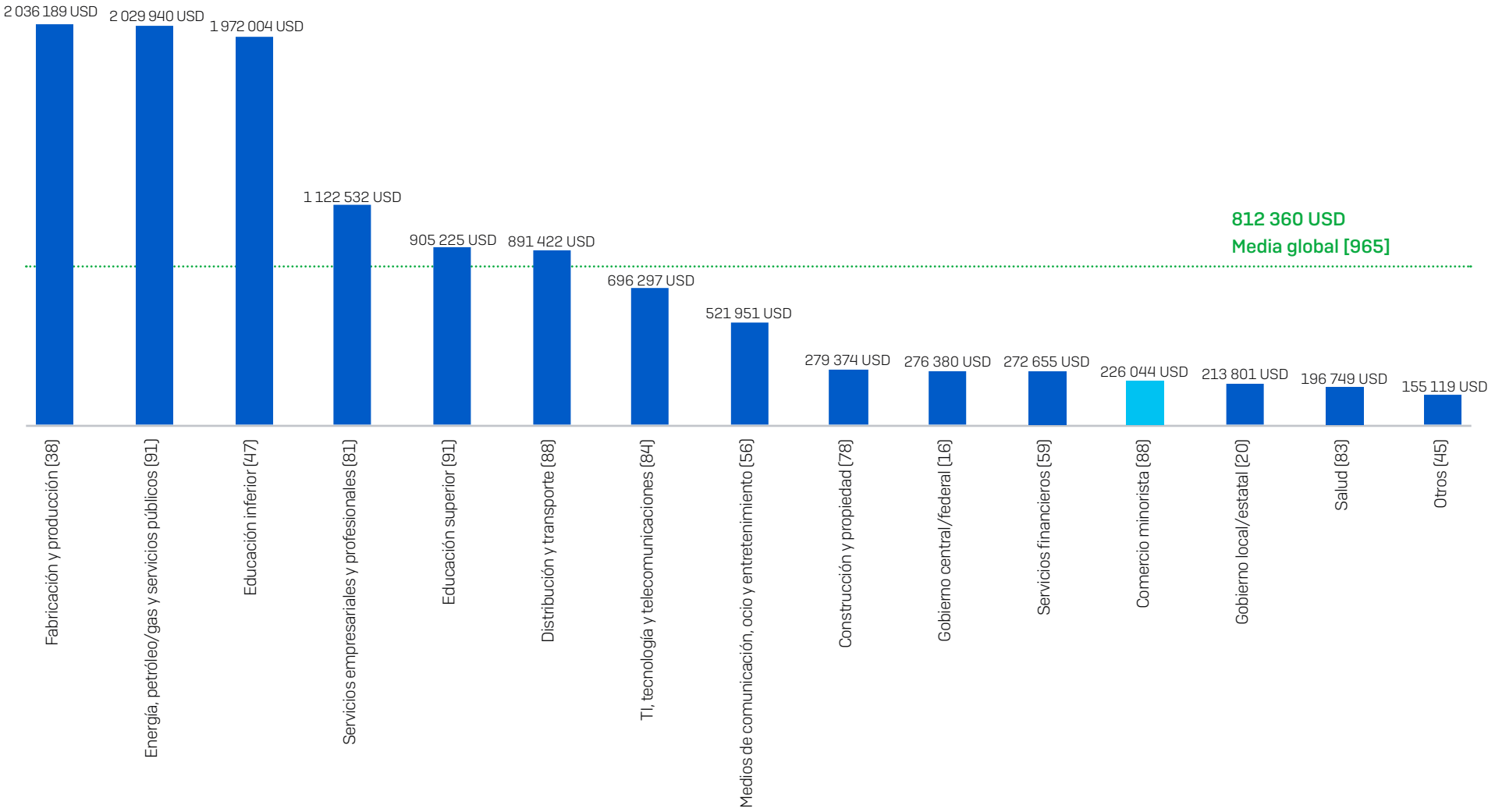


Porcentaje que recuperó TODOS sus datos después de pagar el rescate



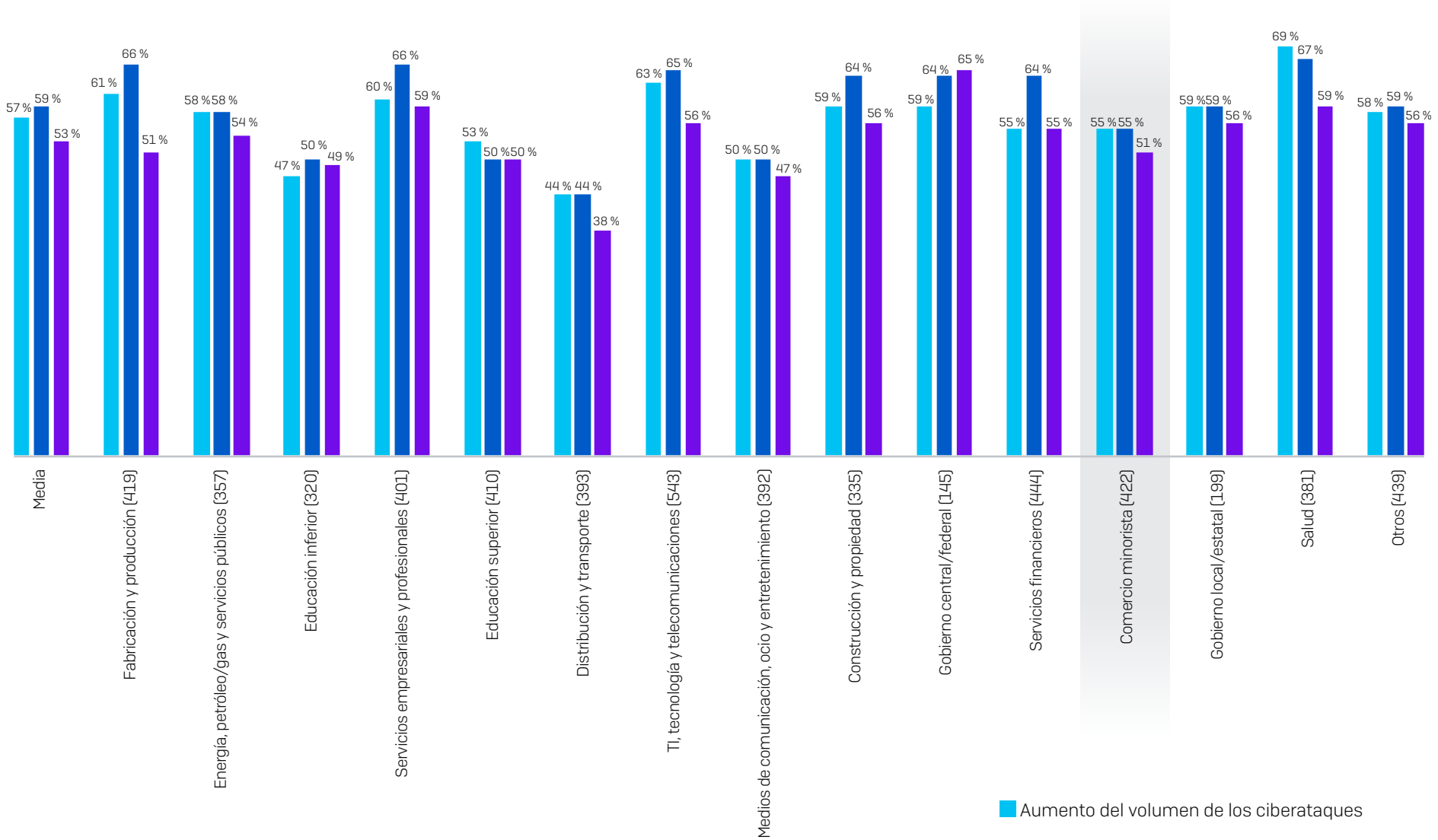
¿Qué proporción de los datos recuperó su organización en el ataque de ransomware más importante?
(109/33 organizaciones minoristas que pagaron el rescate y recuperaron datos)

El importe de rescate en el sector minorista es bajo



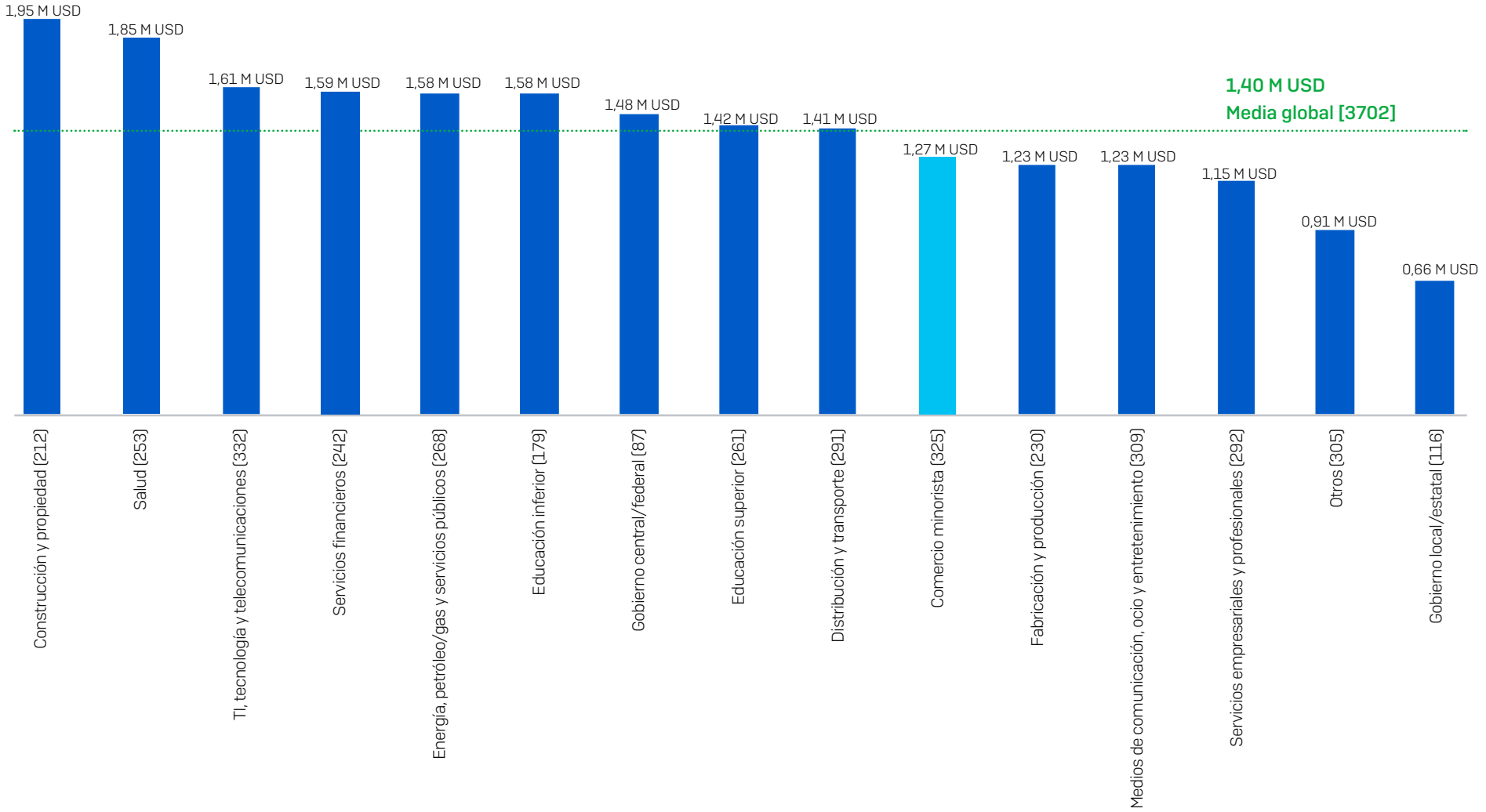
¿Cuál fue el importe del rescate que pagó su organización en el ataque de ransomware más importante? USD. Número base en la tabla. Excluye respuestas "No lo sé". Nota: en el caso de los sectores con números base bajos, el resultado se debe considerar como meramente indicativo.

Posición del sector minorista: cambio en la experiencia con los ciberataques



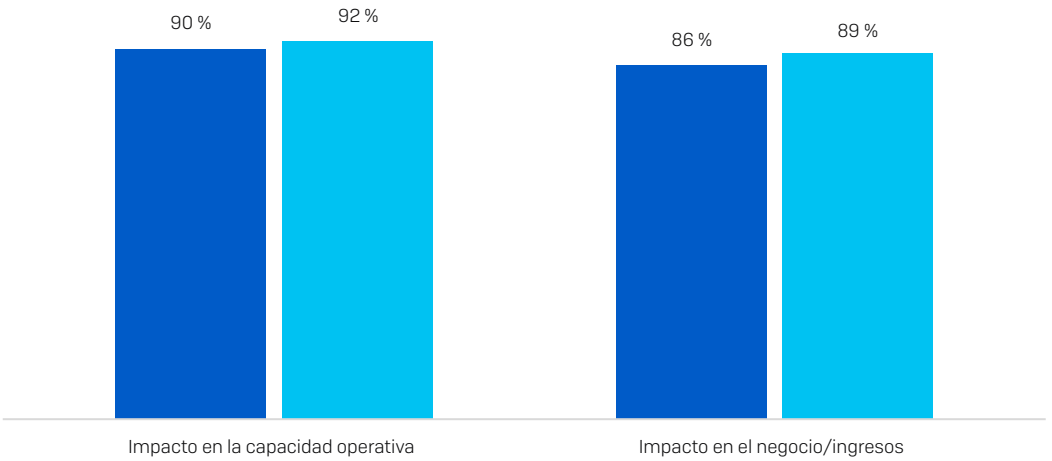
Con respecto al volumen, la complejidad y el impacto, ¿cómo ha cambiado la experiencia de su organización con los ciberataques en el último año? (n=5600 encuestados): Ha aumentado mucho, Ha aumentado un poco

El sector minorista incurre en un coste inferior a la media para rectificar los ataques



¿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.)? (3,702 organizaciones afectadas por el ransomware)

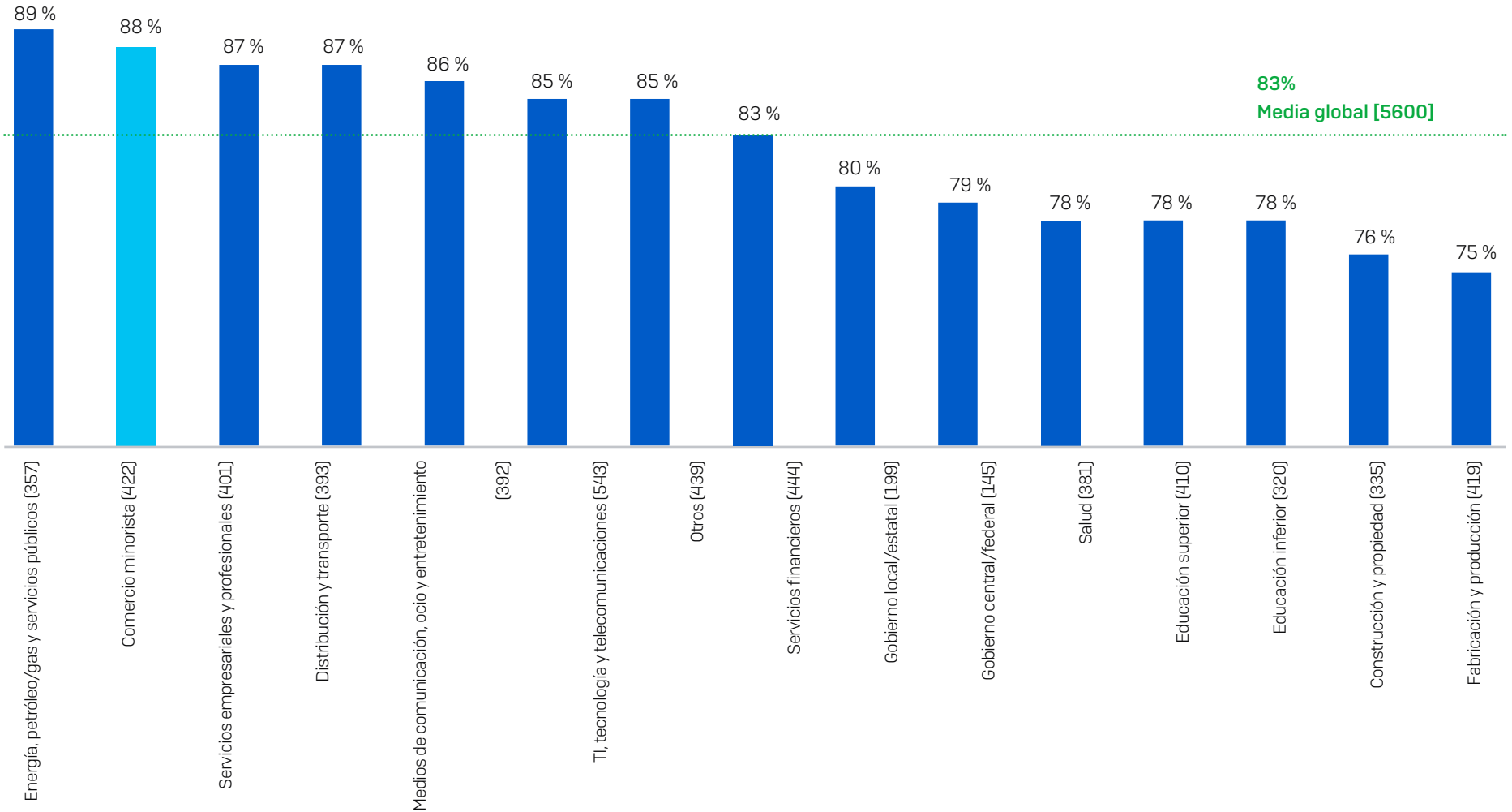
Impacto operativo/comercial del ransomware en el sector minorista



Nota: solo se preguntó a organizaciones del sector privado sobre la pérdida de negocio/ingresos.

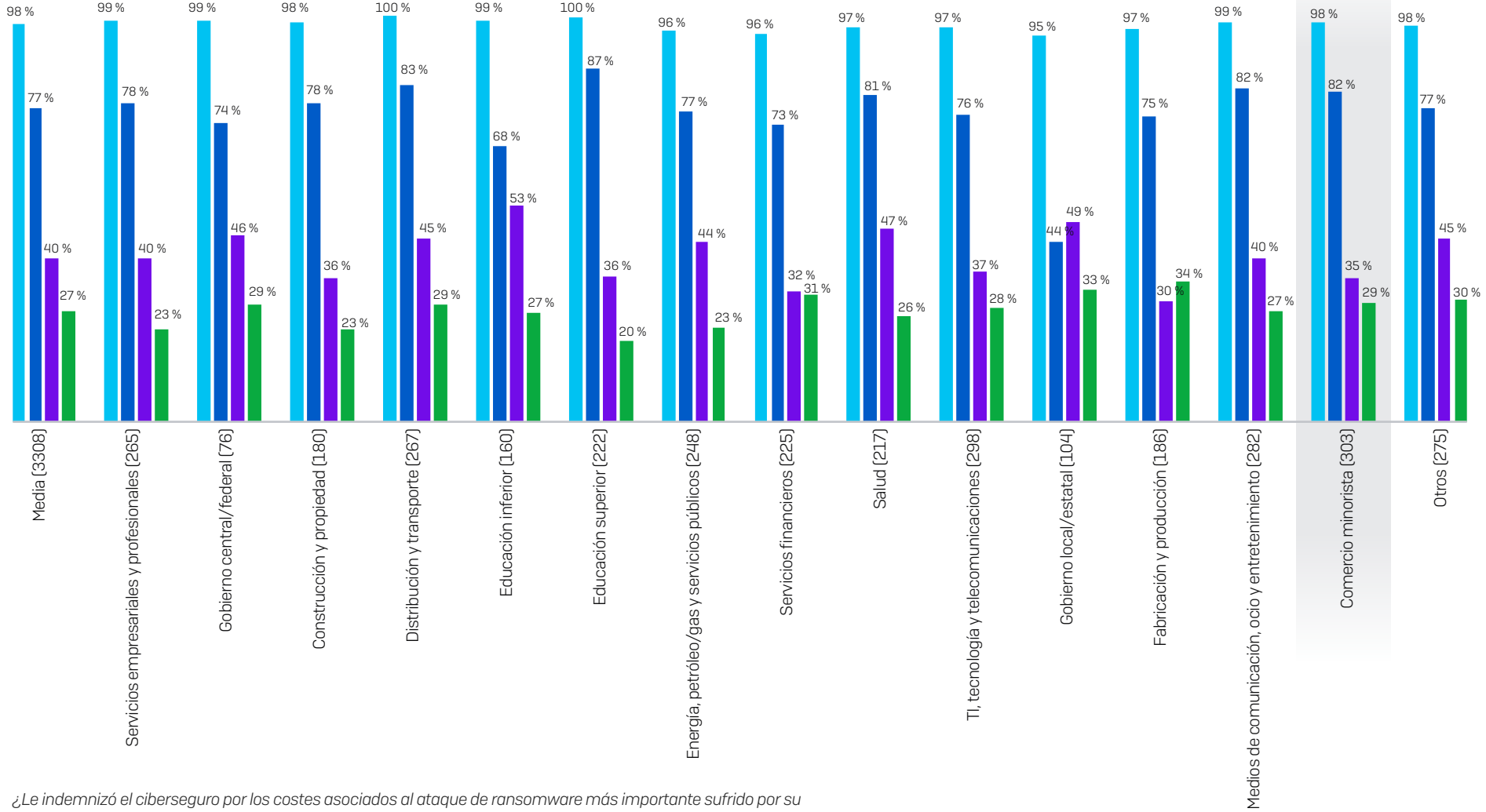
¿Afectó el ataque de ransomware más importante a la capacidad operativa de su organización? ¿Provocó el ataque de ransomware más importante pérdidas de negocio/ingresos a su organización? (n=3702; 325 organizaciones minoristas que se vieron afectadas por el ransomware en el último año) Excluye algunas opciones de respuesta.

El sector minorista tiene el segundo índice más alto de cobertura de ciberseguridad contra el ransomware



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

Posición del sector minorista: tasa de indemnización de los ciberseguros por sector



¿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.

2022-08-25 (WP-ES)

SOPHOS