SOPHOS

El estado del ransomware en el sector educativo 2023

Resultados de una encuesta independiente y desvinculada de cualquier proveedor a 3000 responsables de TI/ciberseguridad en 14 países, incluidos 400 del sector educativo, realizada entre enero y marzo de 2023.

Monográficos de Sophos. Julio de 2023

Introducción

El estudio anual de Sophos sobre las experiencias reales con el ransomware de los responsables de TI/ciberseguridad deja clara la realidad a la que se enfrentan las instituciones educativas en 2023. Revela las causas raíz más comunes de los ataques y arroja nueva luz sobre el impacto del ransomware en el sector educativo. El informe también expone el impacto empresarial y operativo de pagar el rescate para recuperar los datos en lugar de utilizar copias de seguridad.

Acerca de la encuesta

Sophos encargó una encuesta independiente y desvinculada de cualquier proveedor a 3000 responsables de TI/ciberseguridad en organizaciones de entre 100 y 5000 empleados en 14 países de América, EMEA y Asia-Pacífico. La encuesta incluía 400 encuestados del sector educativo: 200 procedentes de instituciones de educación primaria y secundaria (hasta los 18 años) y 200 de educación superior (más de 18 años) e incluía instituciones educativas tanto del sector de público como del privado.

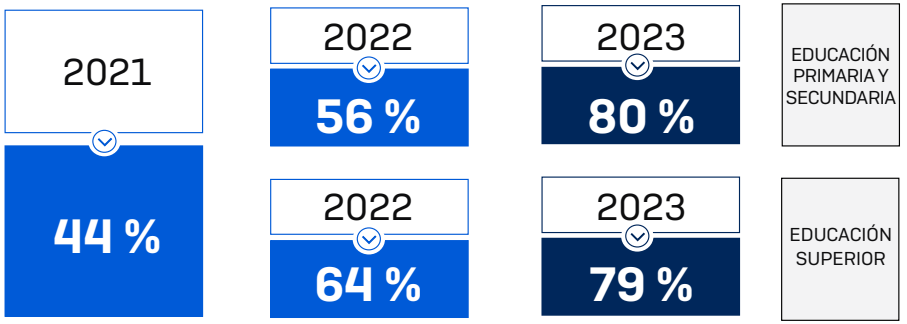
La encuesta se realizó entre enero y marzo de 2023 y a los encuestados se les pidió que respondieran a partir de sus experiencias del año anterior.

Índice de ataques de ransomware en el sector educativo

El estudio de 2023 reveló que el índice de ataques de ransomware en el sector educativo sigue aumentando. El 80 % de las instituciones de educación primaria y el 79 % de las instituciones de educación superior afirmaron haber sido víctimas del ransomware en el último año, comparado con el 56 % y el 64 %, respectivamente, de nuestra encuesta del 2022.

Los índices de ataques de 2023 duplican con creces las cifras de nuestra encuesta de 2021, en que el 44 % de las instituciones educativas (combinando educación primaria y secundaria y educación superior) experimentó un ataque de ransomware. Este importante incremento en el índice de ataques deja claro que los adversarios son ahora capaces de ejecutar sistemáticamente ataques a escala, y podría decirse que el ransomware es el mayor ciberriesgo al que se enfrentan las instituciones educativas hoy día.

Los ciberdelincuentes han ido desarrollando y puliendo el modelo de ransomware como servicio durante varios años. Este modelo operativo reduce la barrera de entrada para los operadores de ransomware en potencia, al tiempo que aumenta la sofisticación de los ataques al permitir la especialización de los adversarios en las diferentes fases de los ataques. Para más información sobre el ransomware como servicio, lea el Informe de Sophos sobre amenazas 2023.



En el último año, ¿su organización ha sido víctima del ransomware? Sí. n=400 (2023), 440 (2022), 499 (2021)

Este año el sector educativo ha registrado los índices más altos de ataques de ransomware de todos los sectores encuestados, lo que sugiere que el sector está especialmente expuesto a los ataques. El sector de TI, tecnología y telecomunicaciones registró el nivel más bajo de ataques (50 %), lo que indica un aumento de la preparación y las defensas en materia cibernética.

El índice creciente de ataques de ransomware en el sector educativo contrasta con la tendencia global en todos los sectores, que se ha mantenido estable: en nuestras encuestas de 2023 y 2022, el 66 % de todos los encuestados afirmó que su organización había sido víctima del ransomware en el año anterior.

Causas raíz de los ataques de ransomware en el sector educativo

La educación primaria y secundaria reveló que el compromiso de credenciales (36 %) y la explotación de vulnerabilidades (29 %) fueron las dos causas raíz principales de los ataques de ransomware. Los correos electrónicos (correos maliciosos o phishing) fueron los puntos de partida en casi un tercio de los ataques (30 %), lo que sugiere que el sector de la educación primaria y secundaria está muy expuesto a las amenazas por correo electrónico.

En la educación superior, la explotación de vulnerabilidades (40 %) fue la causa raíz más común de los ataques de ransomware, y el compromiso de credenciales se situó en segundo lugar con un 37 %. En conjunto, suman más de tres cuartas partes de los ataques de ransomware (77 %) en la educación superior. Los ataques basados en el correo electrónico (correo malicioso o phishing) son una causa raíz menos común, aunque provocan casi uno de cada cinco incidentes de ransomware (19 %).

De todos los grupos de la encuesta, la educación superior fue uno de los sectores que más citaron la explotación de vulnerabilidades como causa raíz de los ataques. Al mismo tiempo, la educación primaria y secundaria fue uno de los sectores con más ataques por compromiso de credenciales.

	EDUCACIÓN PRIMARIA Y SECUNDARIA (n=159)	EDUCACIÓN SUPERIOR (n= 157)	MEDIA DE TODOS LOS SECTORES (n=1974)
Explotación de vulnerabilidades	29 %	40 %	36 %
Compromiso de credenciales	36 %	37 %	29 %
Correo electrónico malicioso	19 %	12 %	18 %
Phishing	11 %	7 %	13 %
Ataque por fuerza bruta	4 %	2 %	3 %
Descargas	1 %	1 %	1 %

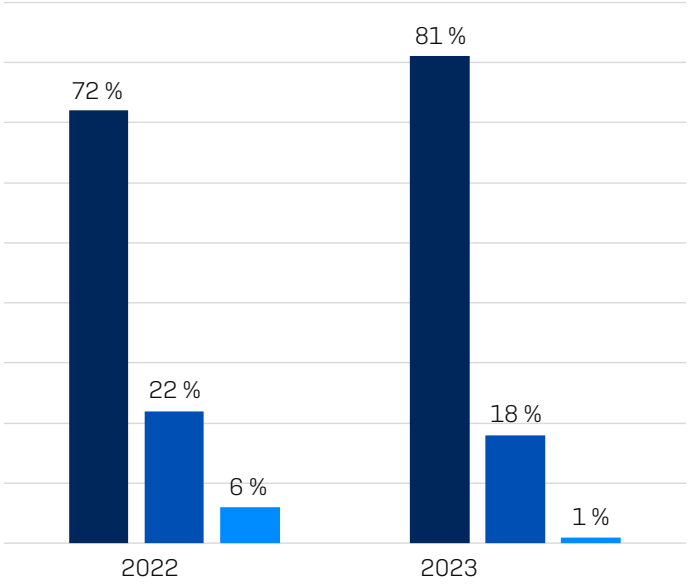
Índice de cifrado de datos en el sector educativo

El cifrado de datos en el sector educativo ha seguido aumentando: el porcentaje de ataques que comportó el cifrado de datos en las instituciones de educación primaria y secundaria ha pasado del 72 % en la encuesta de 2022 al 81 % en la de 2023. En la educación superior, el índice de cifrado de datos registrado en la encuesta de 2023 es del 73 %, similar al 74 % registrado el año anterior. El alto índice de cifrado probablemente refleja el nivel de habilidades cada vez más sofisticado de los adversarios, que continúan innovando y perfeccionando sus métodos.

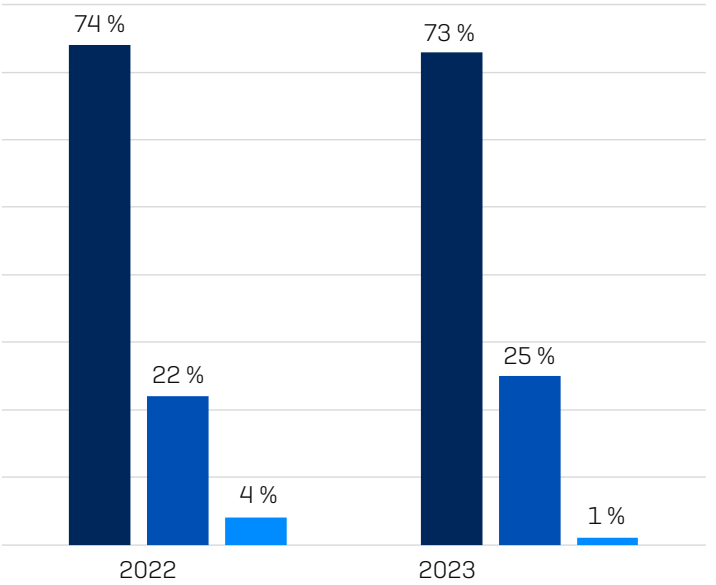
El 18 % de los ataques en la educación primaria y secundaria se detuvieron antes de que los datos se cifraran, lo que supone una disminución comparado con el 22 % en 2022. Sin embargo, la educación superior registró un incremento en el índice de ataques detenidos antes del cifrado de datos, pasando del 22 % en 2022 al 25 % en 2023. El índice de ataques de solo extorsión en las instituciones de educación primaria y secundaria y de educación superior descendió del 5 % en la encuesta del año pasado al 1 % en la de este año.

En todos los sectores, el 76 % de los ataques se saldaron con el cifrado de los datos, y el 21 % se detuvo antes de que los datos se cifraran. La máxima frecuencia del cifrado de datos (92 %) fue registrada por los servicios empresariales y profesionales.

Educación primaria y secundaria



Educación superior



- Sí, se produjo el cifrado de datos
- No, el ataque se detuvo antes de que consiguieran cifrar los datos
- No, los datos no se cifraron pero se pidió un rescate (extorsión)

¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Selección de opciones de respuesta. Educación primaria y secundaria n= 159 (2023), 179 (2022), Educación superior n=157 (2023), 261 (2022)

De las instituciones de educación primaria y secundaria cuyos datos fueron cifrados, el 27 % notificó que también se robaron los datos. Esta cifra se eleva al 35 % en la educación superior. Este enfoque "double dip" de los adversarios cada vez es más común, ya que buscan la manera de incrementar su capacidad de monetizar los ataques. Pueden amenazar con divulgar los datos robados para exigir dinero e incluso vender los datos. La alta frecuencia del robo de datos aumenta la importancia de detener los ataques lo antes posible antes de que se exfiltre la información.

Porcentaje de ataques de ransomware en que se cifraron datos y también se robaron datos

Educación primaria y secundaria	Educación superior
27 %	35 %

¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Sí/Sí, y los datos también se robaron n=128 (educ. primaria y secundaria), 115 (educ. superior)

Índice de recuperación de datos en el sector educativo

Resulta alentador observar que todas las instituciones de educación superior y el 99 % de las de educación primaria y secundaria cuyos datos fueron cifrados pudieron recuperar datos, lo que está por encima de la media de todos los sectores del 97 %.

En la educación primaria y secundaria, el 73 % utilizó copias de seguridad para la recuperación de datos, mientras que casi la mitad (47 %) pagó el rescate. Estas cifras representan una cambio pequeño pero preocupante en comparación con nuestro estudio del 2022, donde el 76 % utilizó copias de seguridad y el 45 % pagó el rescate.

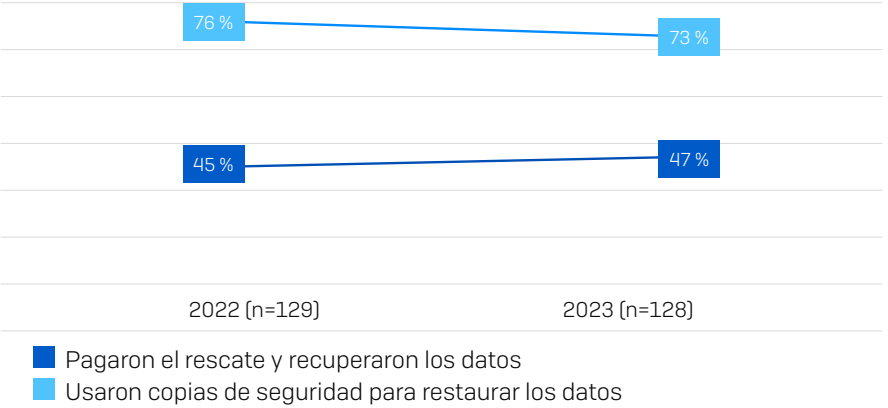
Globalmente, la educación superior se situó entre los tres últimos sectores que utilizaron copias de seguridad: solo dos tercios (63 %) usó las copias de seguridad para recuperar los datos. Solo los sectores de medios de comunicación, ocio y entretenimiento y de distribución y transporte informaron de un menor uso de copias de seguridad. El sector también registró uno de los índices más altos de pagos de rescate para la recuperación de datos: un 56 % pagó para recuperar los datos.

	EDUCACIÓN PRIMARIA Y SECUNDARIA	EDUCACIÓN SUPERIOR	MEDIA DE TODOS LOS SECTORES
Recuperaron datos	99 %	100 %	97 %
Usaron copias de seguridad para restaurar datos	73 %	63 %	70 %
Pagaron el rescate para recuperar datos	47 %	56 %	46 %
Usaron otros medios para recuperar datos	2 %	3 %	2 %

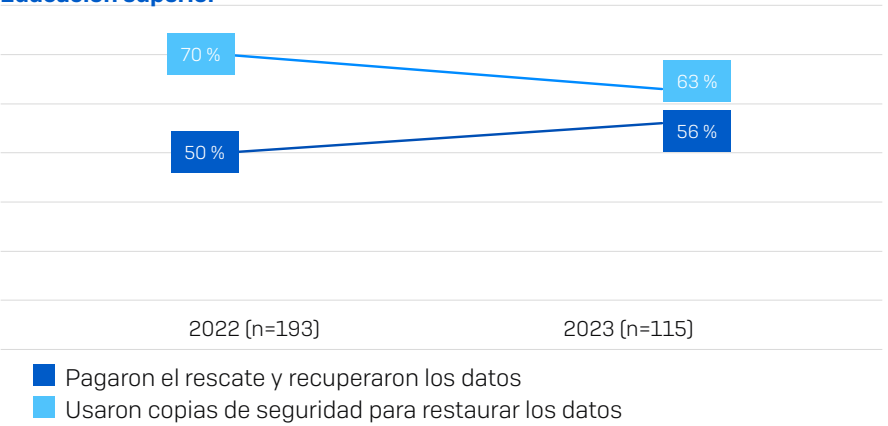
Pagar el rescate y usar copias de seguridad no fueron mutuamente excluyentes, y casi un cuarto de los encuestados del sector educativo (educación primaria y secundaria: 23 %; educación superior: 22 %) afirmó haber utilizado varios medios para recuperar datos cifrados.

Globalmente, el índice de pagos de rescate se ha mantenido estable año tras año en un 46 %, mientras que el uso de copias de seguridad ha descendido del 73 % en el estudio de 2022 al 70 % en el informe de 2023.

Pago de rescates y uso de copias de seguridad para la recuperación de datos: Educación primaria y secundaria



Pago de rescates y uso de copias de seguridad para la recuperación de datos: Educación superior



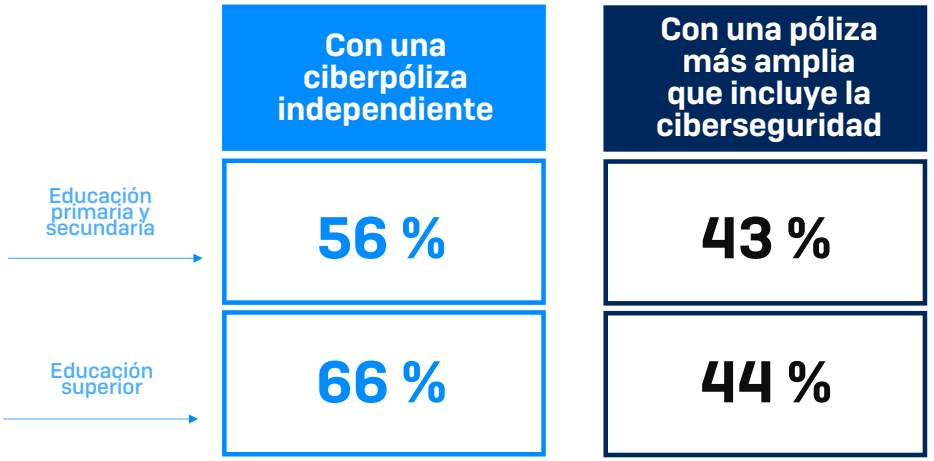
¿Recuperó su organización los datos? Sí, pagamos el rescate y recuperamos datos; Sí, usamos copias de seguridad para restaurar los datos. Números base en la tabla

El impacto de los seguros en la recuperación de datos

Mientras que el índice general de recuperación de datos fue del 99 % en la educación primaria y secundaria y del 100 % en la educación superior, los métodos usados para recuperar los datos variaron según la cobertura del ciberseguro. Las instituciones con pólizas independientes fueron más propensas a pagar el rescate que aquellas con una cláusula de ciberseguridad como parte de una póliza más amplia.

De aquellas cuyos datos se cifraron y tenían una ciberpóliza independiente, el 56 % en la educación primaria y secundaria y el 66 % en la educación superior pagaron el rescate. En cambio, el índice de pago de rescates fue del 43 % (educación primaria y secundaria) y del 44 % (educación superior) para aquellos con pólizas más amplias que incluían una cláusula de ciberseguridad.

Porcentaje de víctimas del ransomware que pagaron el rescate

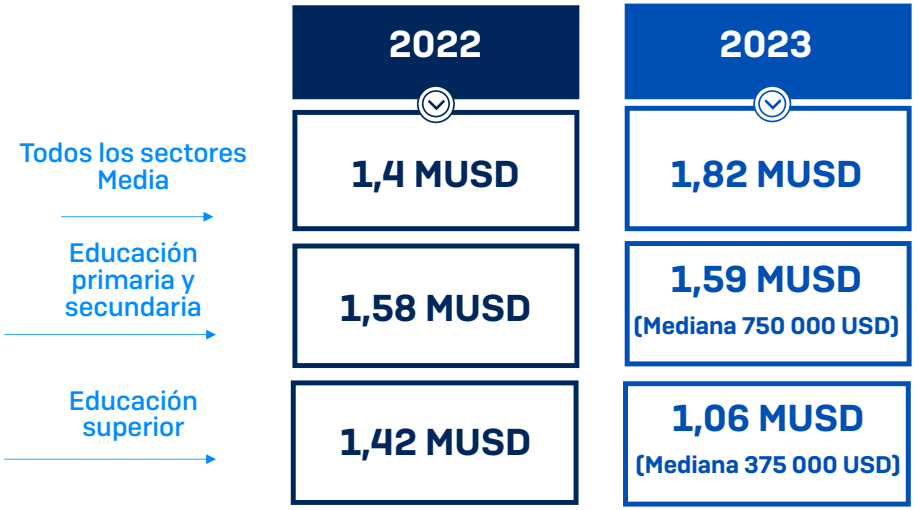


¿Recuperó su organización los datos? Sí, pagamos el rescate y recuperamos datos. n=125 instituciones de educación primaria y secundaria afectadas por el ransomware en el último año y cuyos datos se cifraron (50 con una póliza independiente, 75 con una cláusula de ciberseguridad como parte de una póliza más amplia) n=114 instituciones de educación superior afectadas por el ransomware en el último año y cuyos datos se cifraron (59 con una póliza independiente, 55 con una cláusula de ciberseguridad como parte de una póliza más amplia)

Costes de recuperación

El pago de rescates es solo un elemento de los costes de recuperación en la gestión de los eventos de ransomware. En todos los sectores, excluyendo cualquier rescate pagado, las organizaciones notificaron un coste medio estimado para recuperarse de los ataques de ransomware de 1,82 millones USD, un aumento comparado con la cifra de 1,4 millones USD de 2022 (que incluía el pago de rescates), y en línea con los 1,85 millones USD (incluyendo rescates) indicados en 2021.

Mientras que los costes de recuperación en todos los sectores han aumentado en el último año, en la educación primaria y secundaria se han mantenido estables: 1,59 millones USD en 2023 frente a 1,58 millones USD en 2022). La mediana del coste de recuperación en la educación primaria y secundaria fue de 750 000 USD en 2023. En la educación superior, los costes de recuperación han disminuido considerablemente, pasando de los 1,42 millones USD notificados el año pasado a poco más de 1 millón USD en 2023, y la mediana del coste de recuperación asciende a 375 000 USD.



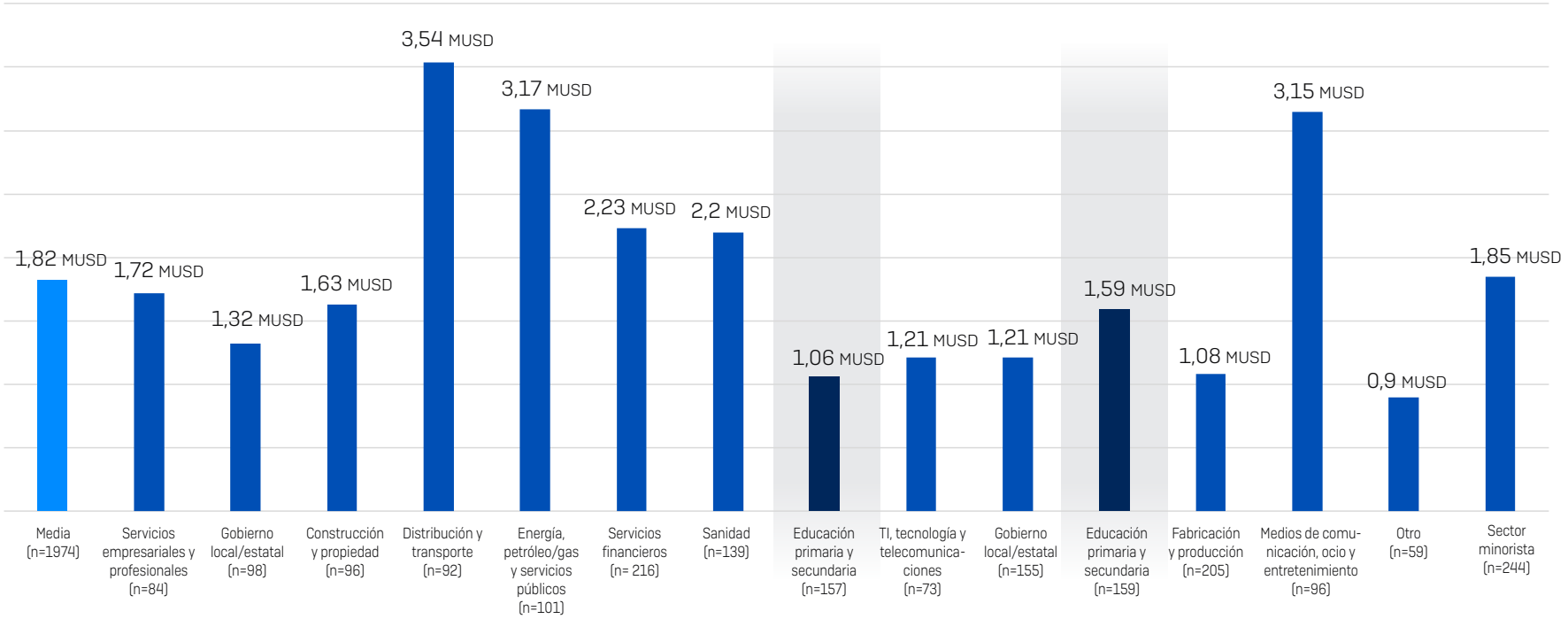
¿Cuál fue el coste aproximado que tuvo que asumir la organización para rectificar los perjuicios del ataque de ransomware más significativo (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, etc.)? Todos los sectores: n=1974 (2023)/3702 (2022); Educación primaria y secundaria: n=159 (2023)/179 (2022); Educación superior: n=157 (2023)/261 (2022)

Nota: el enunciado de la pregunta de 2022 también incluía "pago de rescate".

Esto sugiere que, a medida que el índice de ransomware aumenta, las instituciones de educación superior mejoran progresivamente a la hora de recuperarse de un ataque y lo hacen a un coste más bajo.

Los costes de recuperación en las instituciones educativas fueron mucho más bajos que la media de todos los sectores de 1,82 millones USD. El sector de distribución y transporte pagó los costes de recuperación más elevados (3,54 millones USD), casi el doble de lo que pagaron la mayoría de las demás organizaciones.

Coste de recuperación tras el ataque de ransomware más importante (en millones USD)



¿Cuál fue el coste aproximado que tuvo que asumir la organización para rectificar los perjuicios del ataque de ransomware más significativo (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, etc.)? Números base en la tabla.

Coste de recuperación por método de recuperación de datos

La investigación confirma que las copias de seguridad son la forma más barata de recuperar los datos cifrados frente a pagar el rescate.

En todos los sectores, la mediana del coste de recuperación para las organizaciones que utilizaron copias de seguridad (375 000 USD) es la mitad del de las que pagaron el rescate (750 000 USD). De forma similar, el coste de recuperación medio es de casi 1 millón USD menos para las que usaron copias de seguridad.

Mientras que la educación primaria y secundaria registró un coste de recuperación medio de 1,59 millones USD, para las instituciones que pagaron el rescate el coste se disparó a 2,18 millones USD. En cambio, los costes de recuperación bajaron a 1,37 millones USD para aquellos que usaron copias de seguridad.

En la educación superior, donde el coste de recuperación medio fue de 1,06 millones USD, pagar el rescate tuvo un coste de recuperación de 1,31 millones USD, mientras que el uso de copias de seguridad situó la media del coste de recuperación en algo menos de 1 millones USD.

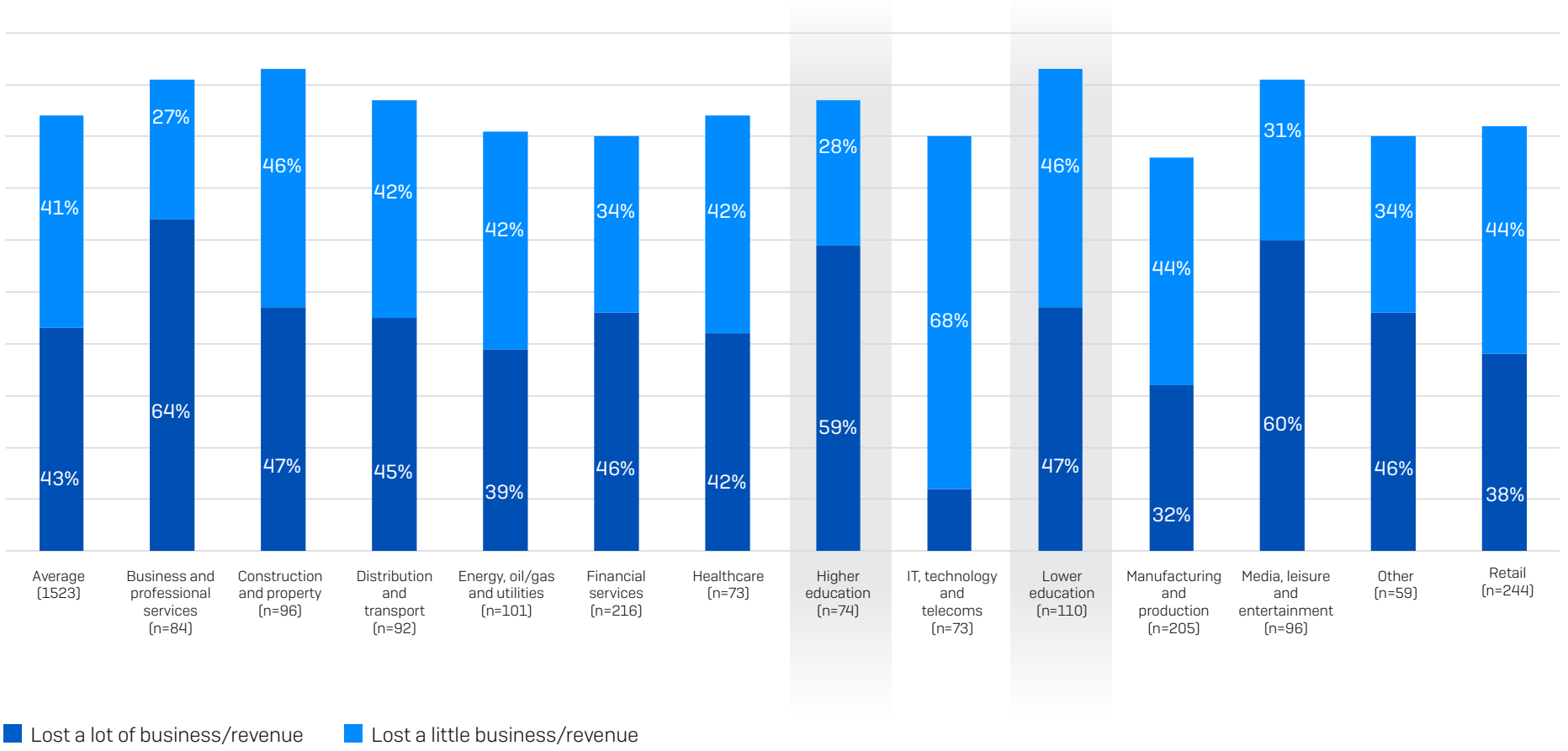
	Pagaron el rescate y recuperaron los datos	Usaron copias de seguridad para restaurar datos
Media de todos los sectores	**2,6 MUSD**	**1,62 MUSD**
Educación primaria y secundaria	**2,18 MUSD**	**1,37 MUSD**
Educación superior	**1,31 MUSD**	**0,98 MUSD**

¿Cuál fue el coste aproximado que tuvo que asumir la organización para rectificar los perjuicios del ataque de ransomware más significativo (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, etc.)? Todos los sectores: n=694 que pagaron el rescate y recuperaron datos y 1053 que usaron copias de seguridad para restaurar los datos;
n=60 (rescate)/94 (copias de seguridad) en educación primaria y secundaria y n=64 (rescate)/73 (copias de seguridad) en educación superior

Impacto empresarial

El sector educativo está particularmente expuesto al impacto del ransomware: las instituciones del sector privado registran algunos de los niveles más altos de pérdida de negocio/ingresos por culpa de un ataque. En general, el 59 % de las instituciones de educación superior afirmaron haber sufrido pérdidas de negocio/ingresos, solo por detrás de los servicios empresariales y profesionales y medios de comunicación, ocio y entretenimiento.

De forma similar, aunque la educación primaria y secundaria registró pérdidas de negocio/ingresos menores, fue el sector más propenso a perder negocio/ingresos (94 %: porcentaje combinado de aquellos que pierden en mayor o menor proporción) debido a un ataque.



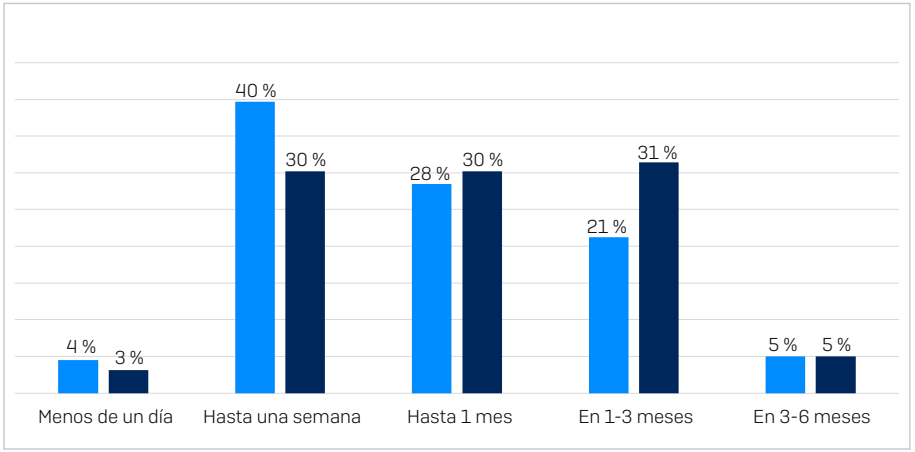
Did the ransomware attack cause your organization to lose business/revenue? Yes, we lost a lot of business/ revenue, Yes, we lost a little business/ revenue.
Private sector organizations that were hit by ransomware, base numbers in chart

Tiempo de recuperación

Las instituciones de educación primaria y secundaria se recuperaron un poco más lentamente de los ataques de ransomware: el 33 % se recuperó en una semana en el estudio de este año frente al 44 % del año pasado. El porcentaje de instituciones que tardaron más de un mes en recuperarse ha subido al 36 % (redondeando) con respecto al 26 % (redondeando) del año anterior, lo que refleja más presiones y un mayor déficit de personal en el sector.

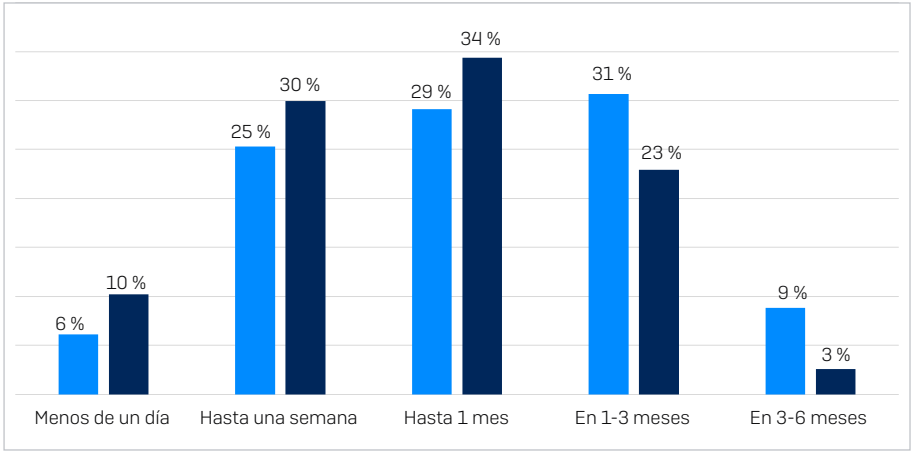
En cambio, la educación superior se recuperó más rápidamente: el 40 % se recuperó completamente en una semana frente al 31 % de la encuesta del año pasado. De forma similar, el porcentaje de las instituciones que tardaron más de un mes en recuperarse descendió del 39 % en el año anterior al 25 % en la encuesta de este año.

Tiempo de recuperación en la educación primaria y secundaria: 2022 frente a 2023



¿Cuánto tiempo tardó su organización en recuperarse totalmente del ataque de ransomware? Números base en la tabla.

Tiempo de recuperación en la educación superior: 2022 frente a 2023



¿Cuánto tiempo tardó su organización en recuperarse totalmente del ataque de ransomware? Números base en la tabla.

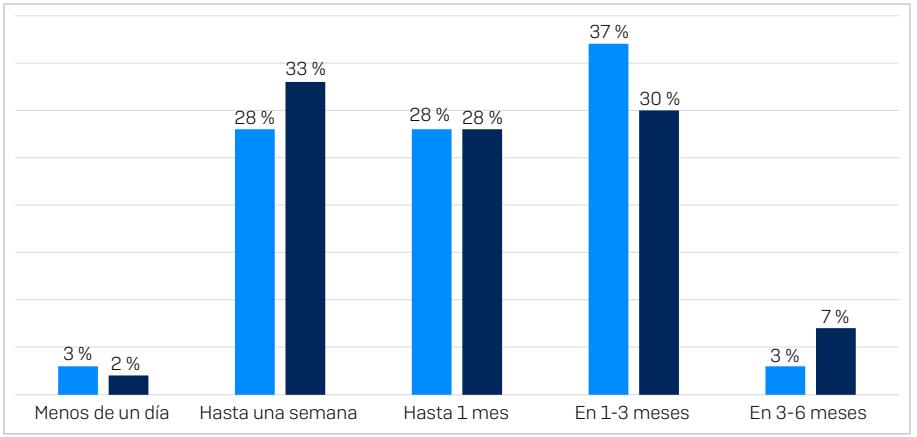
Tiempo de recuperación por método de recuperación de datos

La investigación revela que las instituciones educativas que usan copias de seguridad para recuperar sus datos se reponen de los ataques mucho más rápido que las que pagan el rescate.

Más de un tercio de las instituciones de educación primaria y secundaria que usaron copias de seguridad (35 %) se recuperaron en una semana, comparado con el 32 % de las que pagaron un rescate.

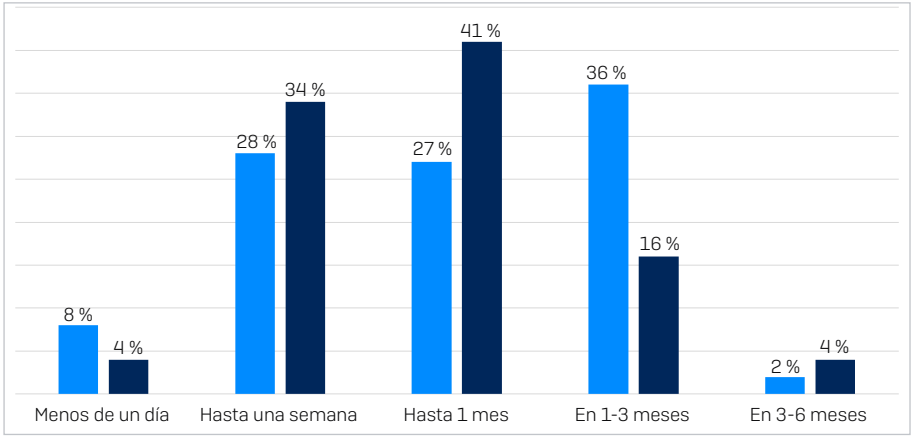
Aunque estas dos opciones de respuesta no se excluían mutuamente y algunos encuestados aplicaron ambos métodos, las ventajas de las copias de seguridad en el proceso de recuperación son evidentes.

Se sigue un patrón similar en la educación superior. El 79 % de los que usaron copias de seguridad se recuperó completamente en un mes, comparado con el 63 % que pagó el rescate. El 38 % de las instituciones que pagó el rescate tardó más de un mes en recuperarse, en comparación con el 21 % de aquellas que usaron copias de seguridad y se recuperaron en ese plazo.



Pagaron el rescate y recuperaron los datos (n=60)
Usaron copias de seguridad para restaurar los datos (n=94)

¿Cuánto tiempo tardó su organización en recuperarse totalmente del ataque de ransomware? Organizaciones que pagaron el rescate y/o usaron copias de seguridad para recuperar los datos. Números base en la tabla



Pagaron el rescate y recuperaron los datos (n=64)
Usaron copias de seguridad para restaurar los datos (n=73)

¿Cuánto tiempo tardó su organización en recuperarse totalmente del ataque de ransomware? Organizaciones que pagaron el rescate y/o usaron copias de seguridad para recuperar los datos. Números base en la tabla

Conclusión

El ransomware sigue siendo una importante amenaza: el sector educativo ha registrado el índice de ataques más alto de todos los sectores en 2023. A medida que los adversarios siguen perfeccionando sus tácticas, técnicas y procedimientos (TTP) de ataque, los responsables de la seguridad luchan por seguir el ritmo, lo que se traduce en mayores índices de cifrado: más de tres cuartas partes de las instituciones educativas (81 % en la educación primaria y secundaria; 73 % en la educación superior) afectadas por el ransomware sufrieron el cifrado de sus datos. Además, el 27 % en educación primaria y secundaria y el 35 % en educación superior declararon que también les robaron datos cifrados.

Resulta preocupante que el uso de copias de seguridad para recuperar los datos cifrados en la educación haya descendido en el último año, mientras que el índice de pago de rescates ha ido aumentado año tras año. De hecho, la educación superior registró uno de los mayores usos de pagos de rescate para la recuperación de datos en la encuesta de 2023. La buena noticia es que todas las instituciones de educación superior (100 %) y el 99 % de las de educación primaria y secundaria cuyos datos fueron cifrados pudieron recuperar datos después del ataque, lo que supera la media de todos los sectores del 97 %.

La posición de las instituciones frente a las aseguradores tuvo un impacto en el método de recuperación de datos en la educación. Los centros educativos con una ciberpóliza independiente fueron más propensos a pagar el rescate para recuperar los datos que los que tenían una cláusula de ciberseguridad incluida en una póliza más amplia.

Las instituciones educativas fueron de las que gastaron menos en recuperarse de un ataque: la educación primaria y secundaria registró un coste de recuperación medio de 1,59 millones USD y la educación superior registró un coste de recuperación de 1,06 millones USD, ambas cifras muy por debajo de la media de todos los sectores de 1,82 millones USD.

Para los centros educativos que operan en el sector privado, el ransomware tiene un gran impacto empresarial. El 94 % de las instituciones de educación primaria y secundaria y el 88 % de las instituciones de educación superior afectadas por el ransomware registraron pérdidas de negocio/ingresos como resultado de los ataques.

Con el crecimiento del modelo de negocio del ransomware como servicio, Sophos no prevé un descenso de los ataques en el próximo año.

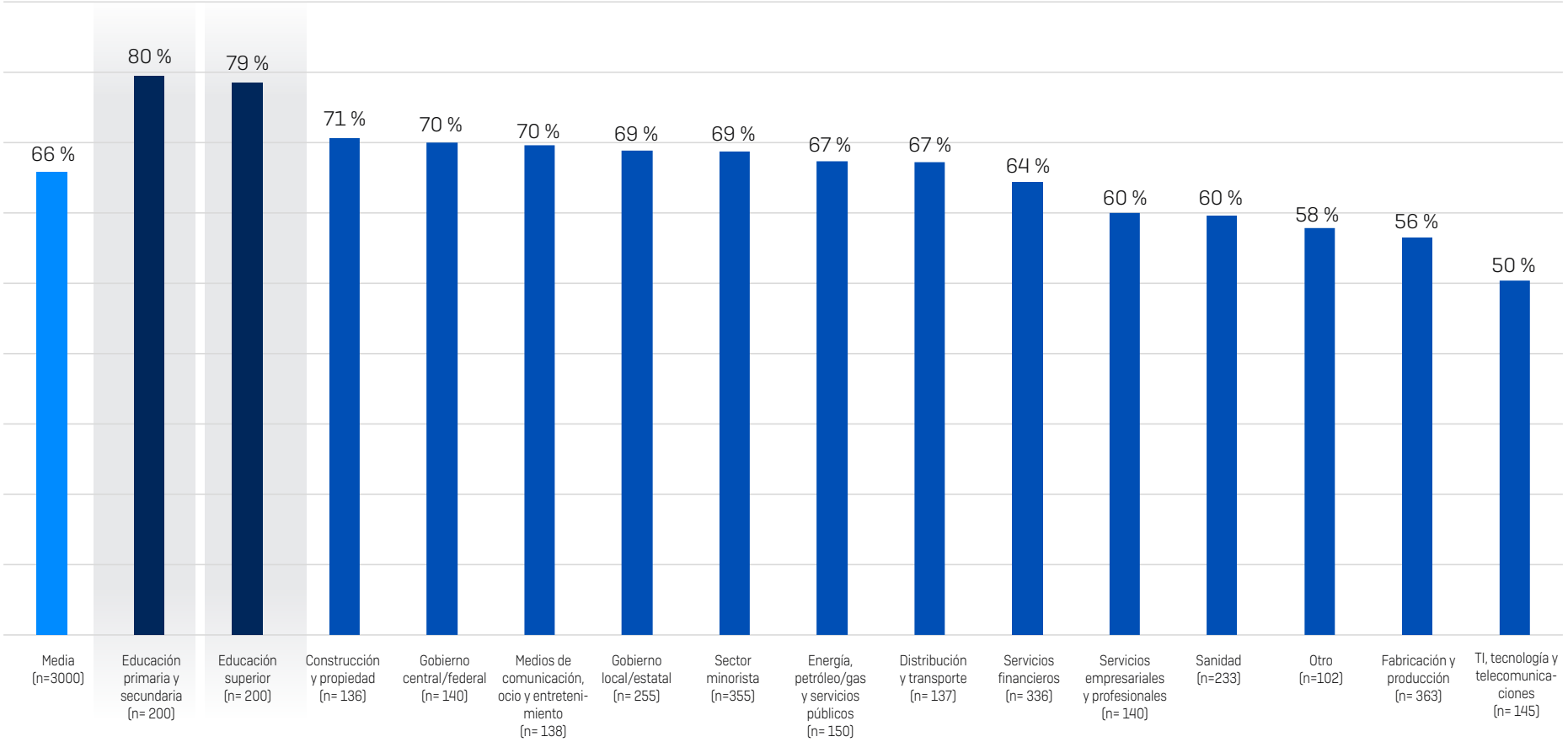
Las organizaciones deben centrarse en:

1. Seguir reforzando sus escudos defensivos con:
    - Herramientas de seguridad para defenderse ante los vectores de ataque más comunes, incluida la protección de endpoints con sólidas funciones antiexploits para evitar la explotación de vulnerabilidades, y Zero Trust Network Access (ZTNA) para prevenir el abuso de credenciales comprometidas.
    - Tecnologías adaptativas que respondan automáticamente a los ataques, desestabilizando a los adversarios y dando tiempo a los responsables de la seguridad para responder.
    - Detección, investigación y respuesta a amenazas 24/7, ya sea internamente o en asociación con un proveedor especializado de servicios de detección y respuesta gestionadas (MDR).
2. Optimizar la preparación ante los ataques, que incluye realizar copias de seguridad con regularidad, practicar la recuperación de datos a partir de copias de seguridad y mantener un plan de respuesta ante incidentes totalmente actualizado.
3. Mantener una buena higiene de seguridad que incluya la aplicación oportuna de parches y la revisión periódica de las configuraciones de las herramientas de seguridad.

Gráficos adicionales

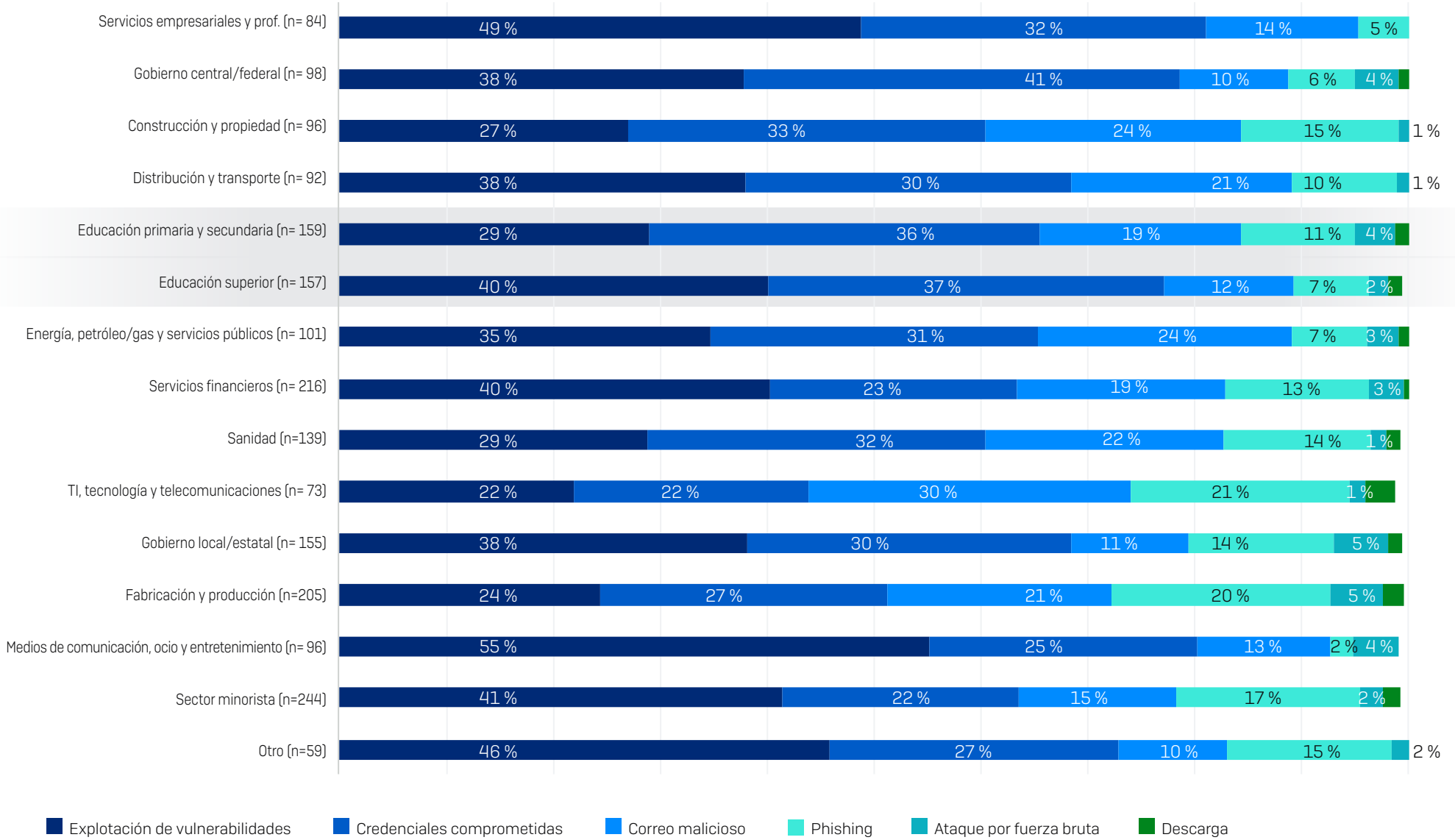
Ataques de ransomware por sector

Porcentaje de organizaciones atacadas por ransomware



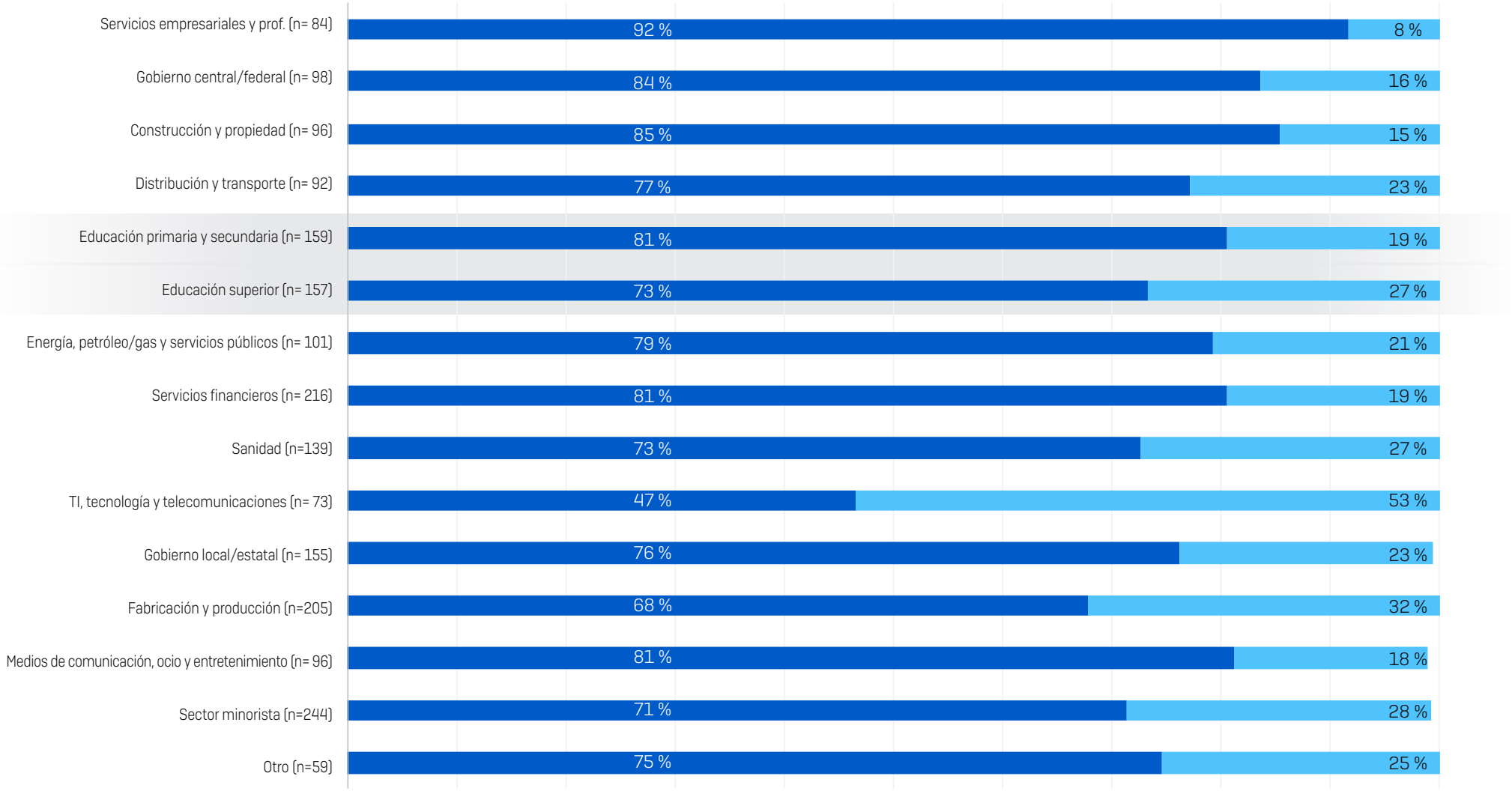
En el último año, ¿se ha visto afectada su organización por el ransomware? Números base en la tabla

Causas raíz del ataque por sector



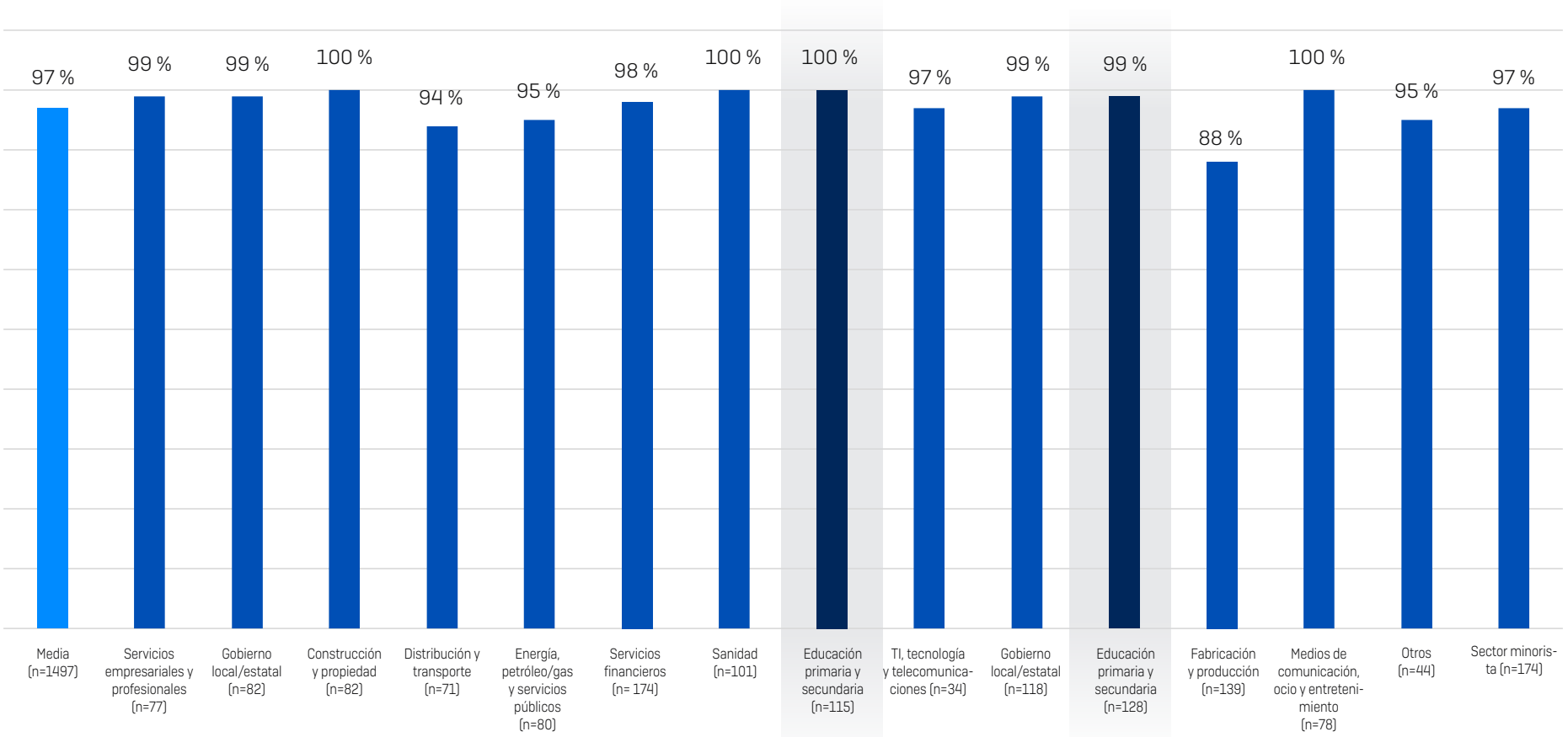
¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? Selección de opciones de respuesta. Números base en la tabla

Cifrado de datos por sector



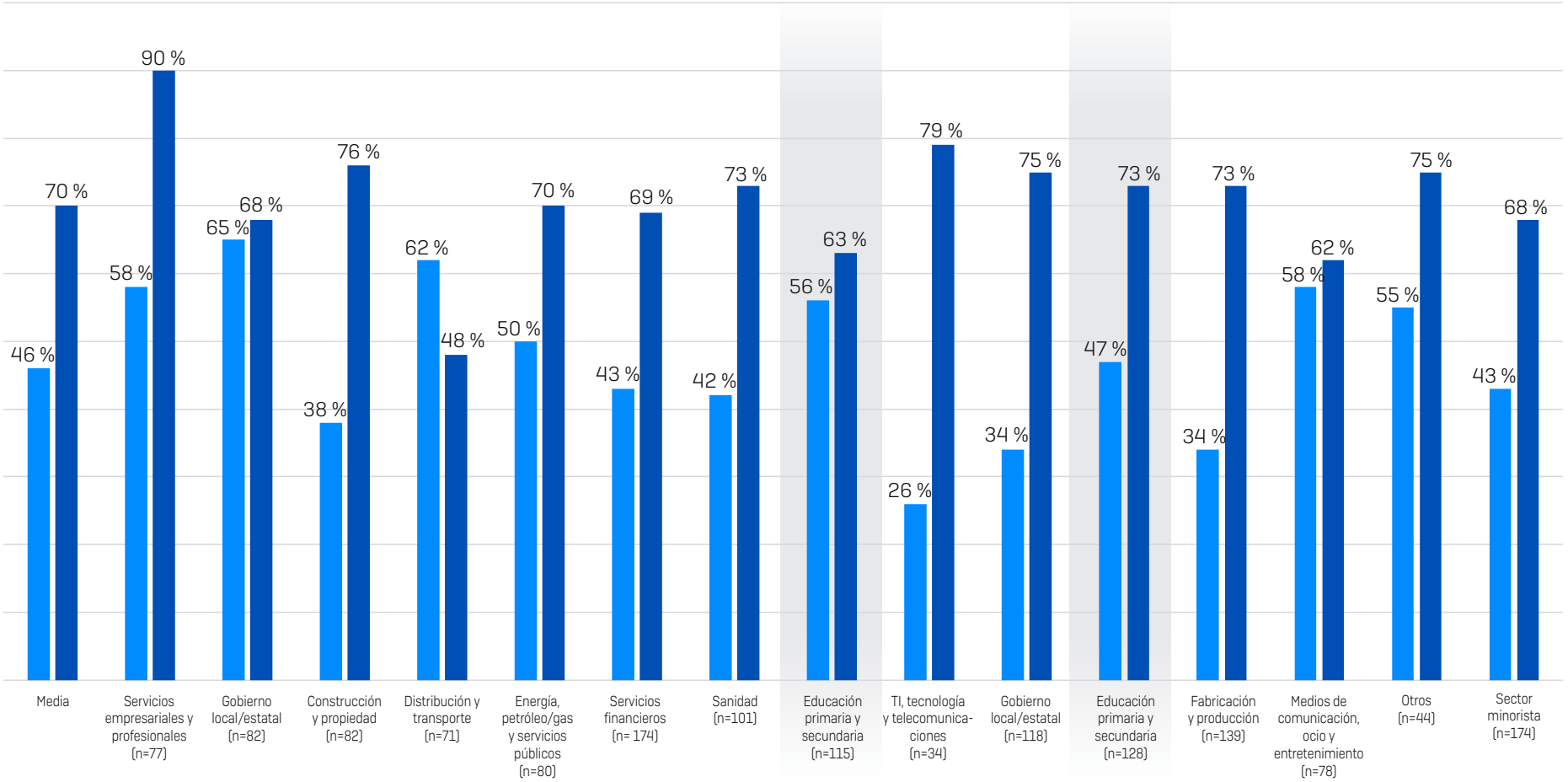
¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Consolidación de opciones de respuesta. Números base en la tabla

Índice de recuperación de datos



¿Recuperó su organización los datos? n=1497 organizaciones afectadas por el ransomware y cuyos datos fueron cifrados

Pago de rescate y uso de copias de seguridad para la recuperación de datos



¿Recuperó su organización los datos? n=1497 organizaciones afectadas por el ransomware y cuyos datos fueron cifrados

Metodología de investigación

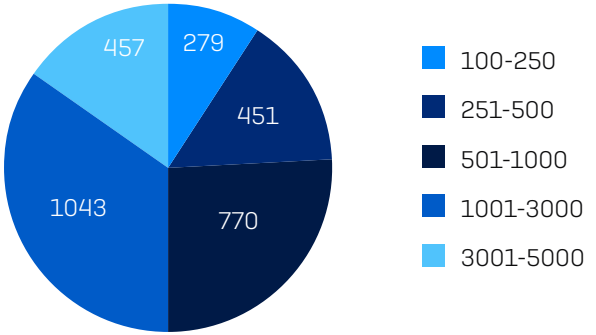
Sophos encargó una encuesta independiente y desvinculada de cualquier proveedor a 3000 responsables de TI/ciberseguridad y se realizó entre enero y marzo de 2023. Los encuestados provenían de 14 países repartidos por América, EMEA y Asia-Pacífico.

Todos los encuestados pertenecían a organizaciones de entre 100 y 5000 empleados (el 50 % de 100-1000 empleados y el otro 50 % de 1001 a 5000 empleados). Dentro del grupo de investigación, los ingresos anuales abarcaban desde menos de 10 millones USD hasta más de 5000 millones USD.

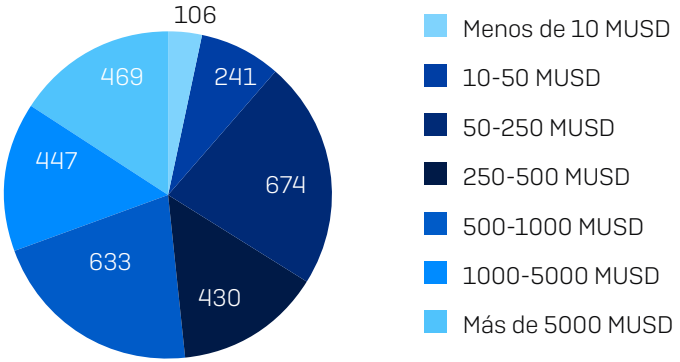
Encuestados por país

PAÍS	NÚMERO DE ENCUESTADOS	PAÍS	NÚMERO DE ENCUESTADOS
Estados Unidos	500	Reino Unido	200
Alemania	300	Sudáfrica	200
India	300	Francia	150
Japón	300	España	150
Australia	200	Austria	100
Brasil	200	Singapur	100
Italia	200	Suiza	100

Encuestados por tamaño de la organización (número de empleados)



Encuestados por tamaño de la organización (ingresos anuales)



Sophos ofrece soluciones de ciberseguridad líderes en el sector a empresas de todos los tamaños, protegiéndolas en tiempo real de amenazas avanzadas como el malware, el ransomware y el phishing. Gracias a nuestras funcionalidades next-gen probadas, los datos de su organización estarán protegidos de forma eficiente por productos con tecnologías de inteligencia artificial y Machine Learning.

2023-07-17 (WP-PS)

SOPHOS