SOPHOS

El estado del ransomware en el sector sanitario 2023

Resultados de una encuesta independiente y desvinculada de cualquier proveedor a 3000 responsables de TI/ciberseguridad en 14 países, incluidos 233 del sector sanitario, realizada entre enero y marzo de 2023.

Monográficos de Sophos. Agosto 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 organizaciones sanitarias en 2023. Revela las causas raíz más comunes de los ataques y arroja nueva luz sobre el impacto del ransomware en este sector. 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, incluidos 233 del sector sanitario, en 14 países de América, EMEA y Asia-Pacífico. 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 sanitario

Nuestro estudio de 2023 revela que el índice de ataques de ransomware en el sector sanitario ha caído del 66 % al 60 % de un año a otro. A pesar de la tendencia a la baja, el índice de ataques del informe de 2023 es casi el doble del registrado en la encuesta de 2021, año en que el 34 % de las organizaciones sanitarias afirmaron haber sido víctimas del ransomware.

Aunque el sector ha registrado una menor frecuencia de ataques, teniendo en cuenta que casi dos tercios de las organizaciones del sector sanitario se vieron afectadas por el ransomware en el último año, está claro que los adversarios son capaces de ejecutar sistemáticamente ataques a escala, lo que hace que el ransomware sea posiblemente el mayor ciberriesgo al que se enfrentan las organizaciones sanitarias hoy en 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.

2021	2022	2023
34 %	66 %	60 %

En el último año, ¿se ha visto afectada su organización por el ransomware? Sí. n=233 (2023), 381 (2022), 328 (2021)

En contraste con el descenso del índice de ataques de ransomware en el sector sanitario, la tendencia global en todos los sectores se mantiene estable: tanto en nuestra encuesta de 2023 como en la de 2022, el 66 % de todos los encuestados afirmaron que sus organizaciones habían sido víctimas de ransomware el año anterior.

De todos los sectores, la educación fue el sector más afectado: un 80 % en educación primaria y secundaria y un 79 % en educación superior sufrieron un ataque. 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.

Causas raíz de los ataques de ransomware en el sector sanitario

El compromiso de credenciales (32 %) fue la causa raíz más común de los ataques de ransomware más significativos en el sector sanitario, seguida de la explotación de vulnerabilidades (29 %). Los ataques basados en el correo electrónico (correo malicioso o phishing) fueron el punto de partida de más de un tercio de los ataques (36 %) en las organizaciones sanitarias, una cifra superior a la media de todos los sectores del 30 %.

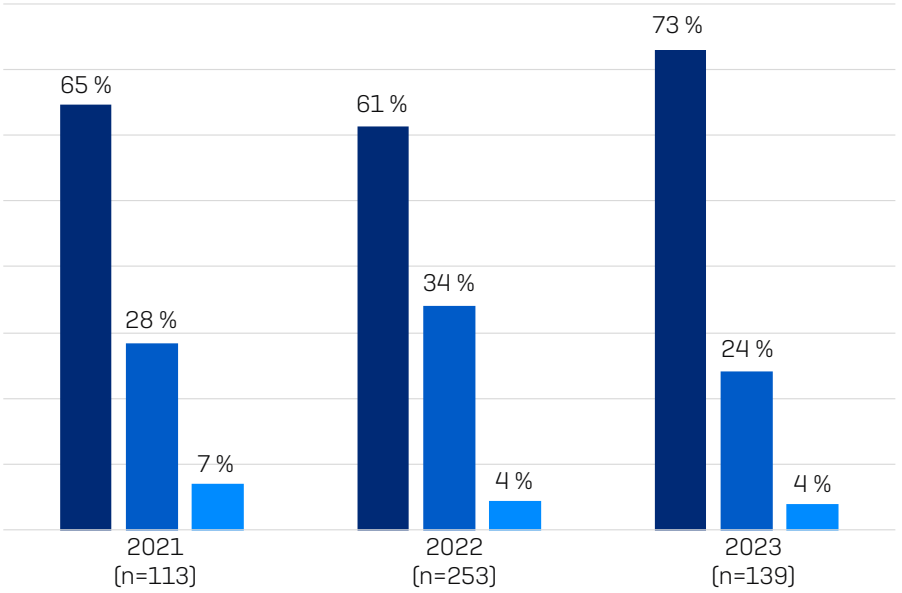
A nivel global e intersectorial, se intercambia el orden de las dos principales causas raíz: la explotación de vulnerabilidades es la más común (utilizada en el 36 % de los ataques), seguida por el compromiso de credenciales (detrás del 29 % de los ataques).

	SANIDAD (n=139)	MEDIA DE TODOS LOS SECTORES (n=1974)
Explotación de vulnerabilidades	29 %	36 %
Compromiso de credenciales	32 %	29 %
Correo electrónico malicioso	22 %	18 %
Phishing	14 %	13 %
Ataque por fuerza bruta	1 %	3 %
Descarga	1 %	1 %

Índice de cifrado de datos en el sector sanitario

El índice de cifrado de datos en el sector sanitario fue el más alto de los últimos tres años de informes, ya que casi tres cuartas partes de las organizaciones sanitarias (73 %) afirmaron que sus datos habían sido cifrados, comparado con el 61 % del informe de 2022 y el 65 % del informe de 2021. Esto probablemente refleja el nivel de habilidades cada vez mayor de los adversarios, que continúan innovando y perfeccionando sus métodos.

El índice de ataques de solo extorsión en el sector sanitario se mantuvo estable en el 4 %, por debajo del 7 % registrado en nuestro estudio de 2021.



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. Números base en la tabla

Aunque elevado, el índice de cifrado de datos registrado por el sector sanitario está por debajo de la media de todos los sectores, donde el 76 % de los ataques conllevaron el cifrado de datos. La máxima frecuencia del cifrado de datos (92 %) fue registrada por los servicios empresariales y profesionales.

En más de un tercio de los ataques en el sector sanitario (37 %) en que se cifraron los datos, también se produjo el robo de los datos. 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 extorsionar 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.

37 %
de los ataques de ransomware contra el sector sanitario en que se cifraron datos también implicaron el robo de datos.

¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware?
Sí/Sí, y los datos también fueron robados; n=101/37

Índice de recuperación de datos en el sector sanitario

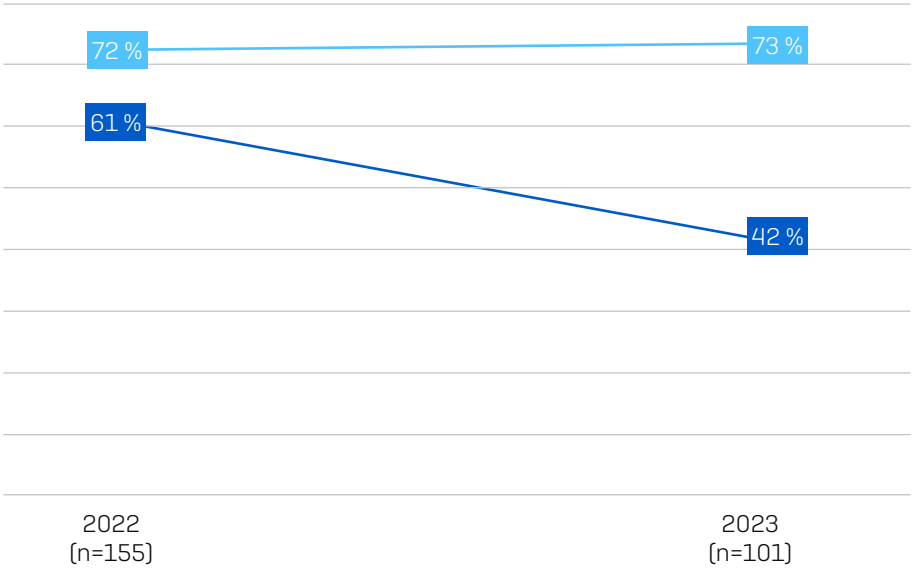
La buena noticia es que todas las organizaciones sanitarias cuyos datos fueron cifrados los recuperaron, por encima de la media de todos los sectores del 97 %.

El 73 % de las organizaciones sanitarias cuyos datos fueron cifrados utilizaron copias de seguridad para recuperarlos, un porcentaje muy ligeramente superior al 72 % registrado en nuestra encuesta de 2022. Resulta alentador observar que ha disminuido la predisposición a pagar el rescate para recuperar los datos cifrados: el 42 % de los encuestados del sector sanitario afirmaron haber pagado el rescate para recuperar los datos, un porcentaje inferior al 61 % del informe del año pasado. El 17 % de los encuestados afirmaron haber utilizado varios medios para recuperar datos cifrados.

	SANIDAD	MEDIA DE TODOS LOS SECTORES
Recuperaron datos	**100 %**	**97 %**
Usaron copias de seguridad para restaurar datos	**73 %**	**70 %**
Pagaron el rescate para recuperar datos	**42 %**	**46 %**
Usaron otros medios para recuperar datos	**2 %**	**2 %**

¿Recuperó su organización los datos? Sí, usamos copias de seguridad para restaurar los datos; Sí, pagamos el rescate y recuperamos datos; Sí, usamos otros medios para recuperar nuestros datos. n=1497 (todos los sectores); n=101 (sector sanitario).

El índice de pago de rescates en el sector sanitario no solo fue significativamente inferior al del año anterior, sino que también se situó por debajo de la media de todos los sectores, que fue del 46 %. Globalmente, el índice de pagos de rescate se ha mantenido estable año tras año, mientras que el uso de las copias de seguridad descendió del 73 % del estudio de 2022 al 70 % del informe de 2023.



¿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 propensión a pagar el rescate

Mientras que el índice general de recuperación de datos en las organizaciones sanitarias fue del 100 %, los métodos usados para recuperar los datos variaron en función de la cobertura del ciberseguro. Las organizaciones con pólizas independientes fueron más propensas a pagar el rescate que aquellas con una cláusula de ciberseguridad como parte de una póliza más amplia.

Más de la mitad de las organizaciones sanitarias (53 %) cuyos datos fueron cifrados y tenían una ciberpóliza independiente pagaron el rescate. Esta cifra disminuyó al 34 % en las organizaciones con pólizas más amplias que incluían una cláusula de ciberseguridad.

Impacto de los seguros en el pago de un rescate en el sector sanitario

Ciberpóliza independiente	Una póliza más amplia que incluye la ciberseguridad
53 % pagaron el rescate	**34 %** pagaron el rescate

¿Recuperó su organización los datos? Sí, pagamos el rescate y recuperamos datos. n=101 organizaciones sanitarias afectadas por el ransomware en el último año y cuyos datos fueron cifrados (45 con una ciberpóliza independiente, 53 con una cláusula de ciberseguridad como parte de una póliza más amplia).

Pagos de rescate

Mientras que la predisposición general a pagar el rescate se mantiene en el mismo nivel que en el estudio del año anterior, los pagos en sí han aumentado considerablemente a nivel global e intersectorial: el importe de rescate medio casi se ha duplicado, pasando de 812 360 USD a 1 542 330 USD de un año a otro. Con respecto a 2022, la mediana del importe de rescate ha aumentado de 76 500 a 400 000 USD.

En el caso del sector sanitario, 12 organizaciones compartieron la cantidad exacta del rescate que pagaron, siendo la mediana de 2,5 millones USD, un aumento con respecto a los 30 000 USD de 2022.

Nueve organizaciones sanitarias manifestaron haber pagado rescates de 1 millón USD o más, y solo una pagó menos de 100 000 USD. Aunque el número base bajo significa que los datos del informe de 2023 no son estadísticamente significativos (por lo que deben utilizarse con precaución), los resultados indican que los pagos de rescates en el sector sanitario están aumentando.

	2022	2023
Media de todos los sectores	812 360 USD (media) 76 500 USD (mediana)	1 542 330 USD (media) 400 000 USD (mediana)
Sanidad	196 749 USD (media) 30 000 USD (mediana)	2 884 167 USD (media) 2 500 000 USD (mediana)

¿Cuál fue el importe del rescate que pagó su organización a los atacantes? Excluye respuestas "No lo sé" y casos atípicos. Todos los sectores: n=216 (2023)/ 965 (2022); Sector sanitario: n=12 (2023)/ 83 (2022).

* Los números base del sector sanitario en el estudio de 2023 son bajos, de modo que los resultados deben considerarse orientativos.

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 de 1,82 millones USD para recuperarse de los ataques de ransomware, un aumento comparado con la cifra del informe de 2022 (que incluía el pago de rescates) de 1,4 millones USD, y en línea con los 1,85 millones USD (incluyendo rescates) indicados en el informe de 2021.

Siguiendo la tendencia global, los costes de recuperación de las organizaciones sanitarias han aumentado de 1,85 millones USD a 2,20 millones USD de un año a otro, y casi duplican los 1,27 millones USD registrados por el sector en nuestra encuesta de 2021. Es probable que el incremento de los costes de recuperación en el sector sanitario este año se deba al aumento de la frecuencia del cifrado de datos en los ataques de ransomware.

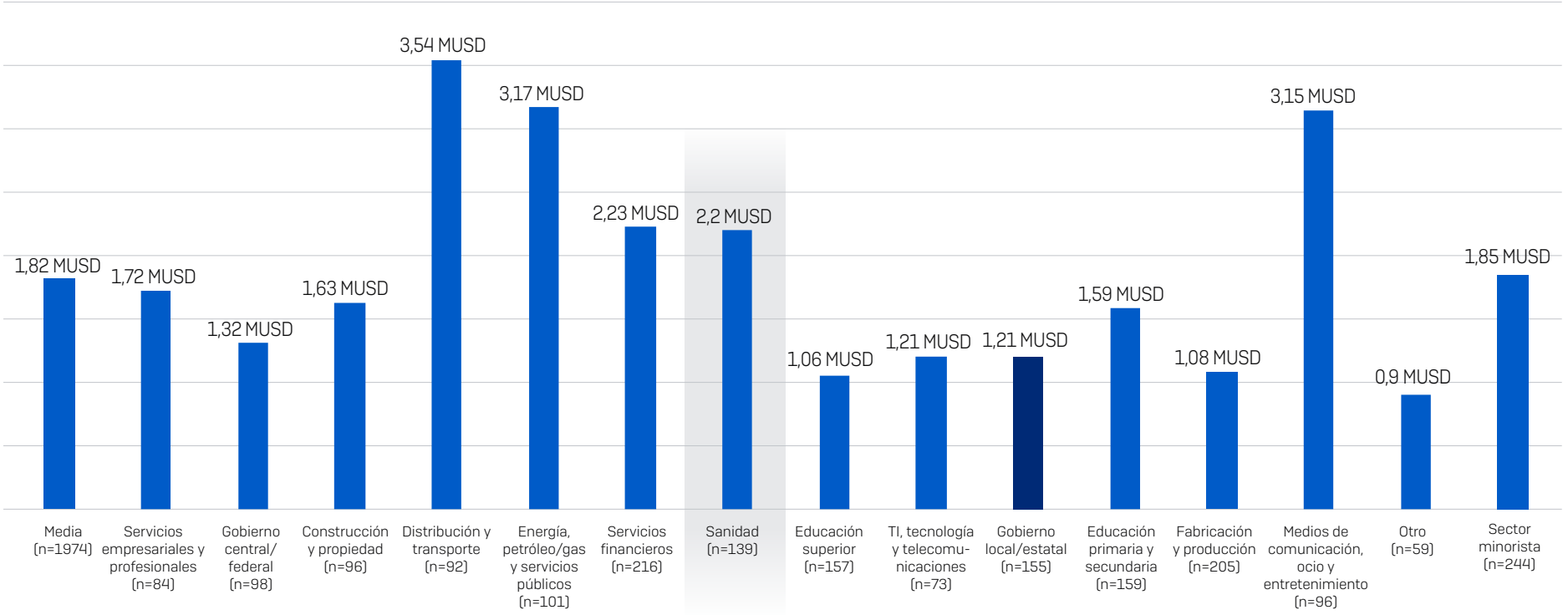
	2021	2022	2023
Media de todos los sectores	1,85 MUSD	1,4 MUSD	1,82 MUSD
Sanidad	1,27 MUSD	1,85 MUSD	2,20 MUSD

¿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=1974 (2023) / 3702 (2022) / 2006 (2021); Sector sanitario: n=139 (2023) / 253 (2022) / 113 (2021)

Nota: el enunciado de la pregunta en las encuestas de 2022 y 2021 también incluía "pago de rescate".

Los costes de recuperación en las organizaciones sanitarias fueron superiores a la media de todos los sectores de 1,82 millones USD. La distribución y el transporte pagaron los costes de recuperación más elevados (3,54 millones USD), casi el doble que la media global.

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 sale mucho más a cuenta recuperar datos cifrados usando copias de seguridad que pagando el rescate.

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

La misma tendencia se ha observado en el sector sanitario, donde el coste de recuperación medio para aquellos que utilizaron copias de seguridad (2,11 millones USD) fue inferior a la factura en la que incurrieron los que pagaron el rescate (2,58 millones USD).

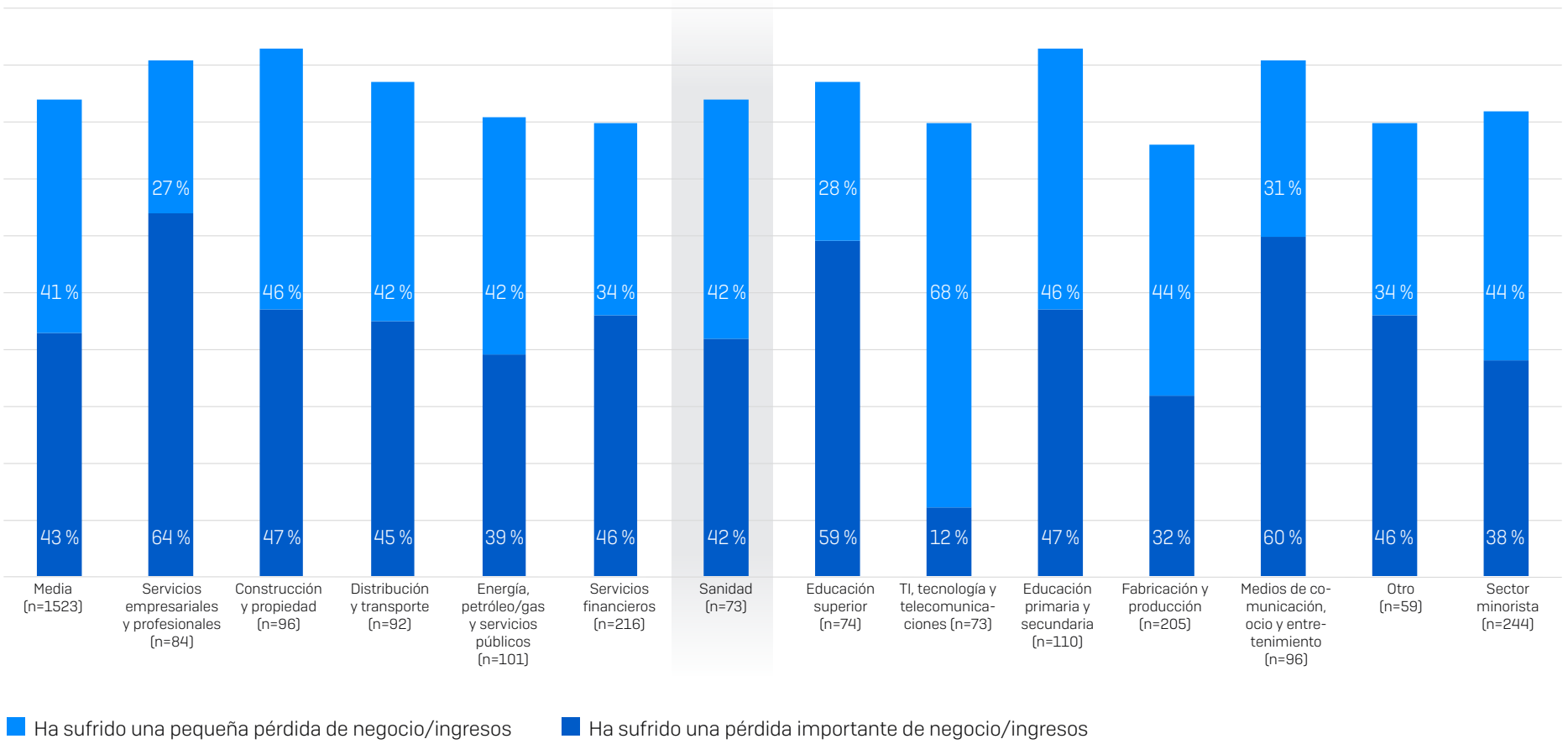
	Pagaron el rescate y recuperaron los datos	Usaron copias de seguridad para restaurar datos
Media de todos los sectores	**750 000 USD** mediana **2,6 MUSD** media	**375 000 USD** mediana **1,62 MUSD** media
Sanidad	**750 000 USD** mediana **2,58 MUSD** media	**750 000 USD** mediana **2,11 MUSD** media

¿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 los datos y 1053 que utilizaron copias de seguridad para restaurar los datos;

Sector sanitario: n=42 que pagaron el rescate y recuperaron los datos y n=74 que utilizaron copias de seguridad para restaurar los datos.

Impacto empresarial

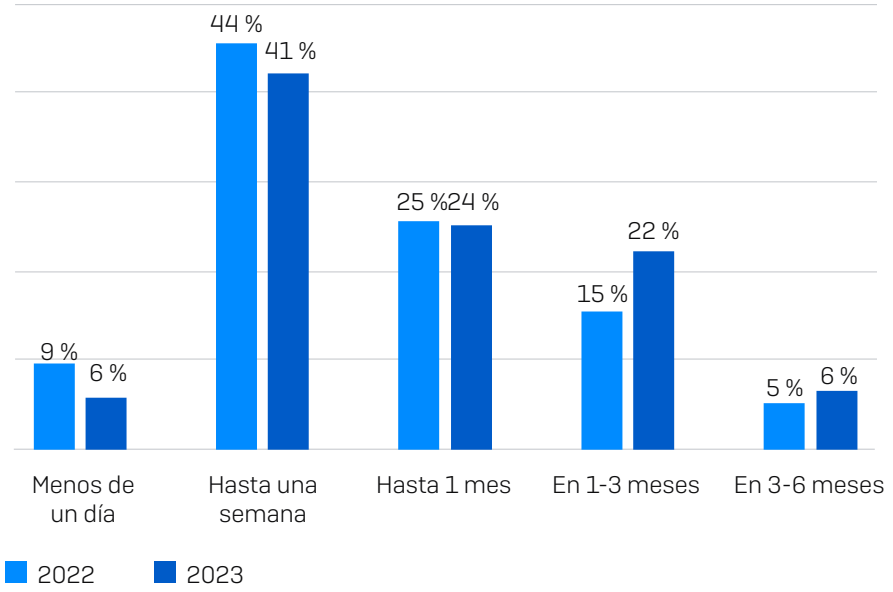
El 85 % de las organizaciones sanitarias del sector privado afectadas por el ransomware afirmaron que el ataque les ocasionó pérdidas de negocio/ingresos, ligeramente por encima de la media global de todos los sectores, que fue del 84 %. Los sectores de la enseñanza primaria y secundaria (94 %) y la construcción y la propiedad (93 %) fueron los más propensos a declarar una pérdida de negocio/ingresos, mientras que los servicios empresariales y profesionales mostraron una mayor disposición a afirmar que habían perdido mucho negocio/ingresos (64 %). Por el contrario, en TI, tecnología y telecomunicaciones, un sector mejor preparado, solo el 12 % manifestó haber perdido mucho negocio/ingresos.



¿El ataque de ransomware provocó pérdidas de negocio/ingresos a su organización? Sí, sufrimos una pérdida importante de negocio/ingresos; Sí, sufrimos una pequeña pérdida de negocio/ingresos. Las organizaciones del sector privado que se vieron afectadas por el ransomware, números base en el gráfico

Tiempo de recuperación

Actualmente, las organizaciones sanitarias tardan más en recuperarse de un ataque de ransomware: el 47 % se recupera en una semana, frente al 54 % registrado en el informe de 2022. Además, el porcentaje de organizaciones que tardaron más de un mes en recuperarse aumentó hasta el 28 % (redondeando) con respecto al 20 % (redondeando) del año anterior.



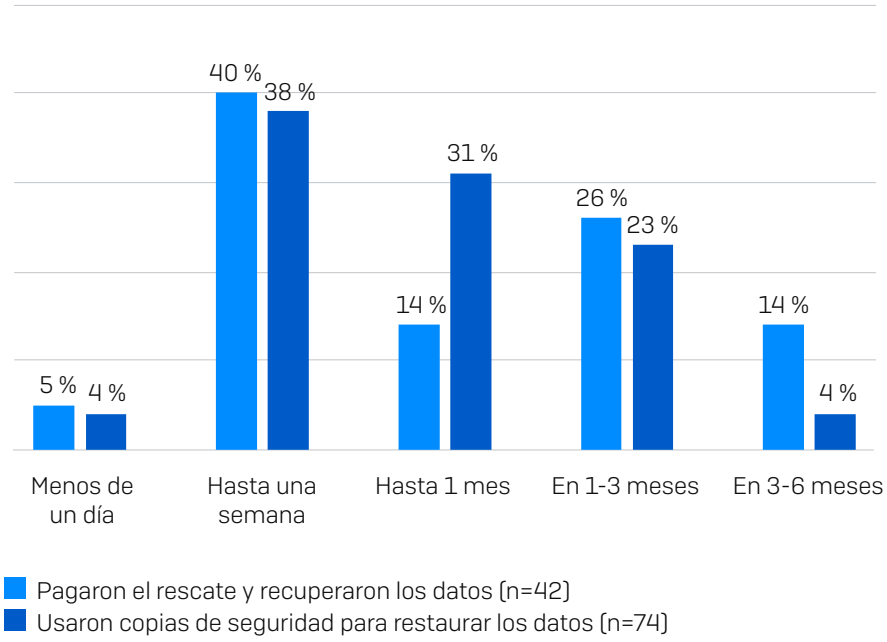
¿Cuánto tiempo tardó su organización en recuperarse totalmente del ataque de ransomware?
139 (en 2023) / 253 (en 2022) organizaciones sanitarias que se vieron afectadas por el ransomware.

Tiempo de recuperación por método de recuperación de datos

La investigación reveló que las organizaciones sanitarias que usan copias de seguridad para restaurar sus datos se reponen del ataque mucho más rápido que las que pagan el rescate.

Una cuarta parte de los encuestados (27 % redondeando) que utilizaron copias de seguridad tardaron más de un mes en recuperar los datos, mientras que el 40 % (redondeando) que pagaron el rescate tardaron más de un mes en recuperarlos.

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.



¿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 amenaza importante para las organizaciones sanitarias. Aunque el sector ha registrado un descenso en el índice de ataques de ransomware en el informe de este año, casi dos tercios (60 %) de los encuestados se vieron afectados por el ransomware.

A medida que los adversarios siguen perfeccionando sus tácticas, técnicas y procedimientos (TTP) de ataque, los responsables de la seguridad apenas consiguen seguirles el ritmo, lo que se traduce en unos niveles de ataque sistemáticamente elevados y en un incremento de los índices de cifrado: casi tres cuartas partes de las organizaciones sanitarias (73 %) afectadas por el ransomware sufrieron el cifrado de sus datos, lo que supone un aumento con respecto al 61 % del año anterior. Además, el 37 % de las organizaciones cuyos datos fueron cifrados notificaron que también se robaron datos.

Como nota alentadora, el sector sanitario registró un descenso en la predisposición a pagar el rescate para recuperar los datos cifrados, pasando del 61 % en la encuesta del año pasado al 42 % en la de 2023.

Al mismo tiempo, el uso de copias de seguridad por parte del sector sanitario solo aumentó ligeramente, del 72 % al 73 % de un año a otro. La buena noticia es que todas las organizaciones sanitarias cuyos datos fueron cifrados pudieron recuperarlos tras el ataque, una cifra superior a la media de todos los sectores del 97 %.

La posición de las organizaciones frente a las aseguradoras tuvo un impacto en su método de recuperación de datos. Mientras que el 53 % de las organizaciones sanitarias cuyos datos fueron cifrados y que tenían una ciberpóliza independiente pagaron el rescate, la cifra descendió al 34 % en el caso de las organizaciones con pólizas más amplias que incluían una cláusula de ciberseguridad.

El coste total de recuperación para las organizaciones sanitarias ha aumentado de 1,85 millones USD a 2,20 millones USD de un año a otro, probablemente y en parte debido al aumento del índice de cifrado tras los ataques. El coste de recuperación del sector sanitario fue superior a la media de todos los sectores de 1,82 millones USD.

Con el crecimiento del modelo de negocio del ransomware como servicio, Sophos no prevé un descenso de los ataques a lo largo del 2023.

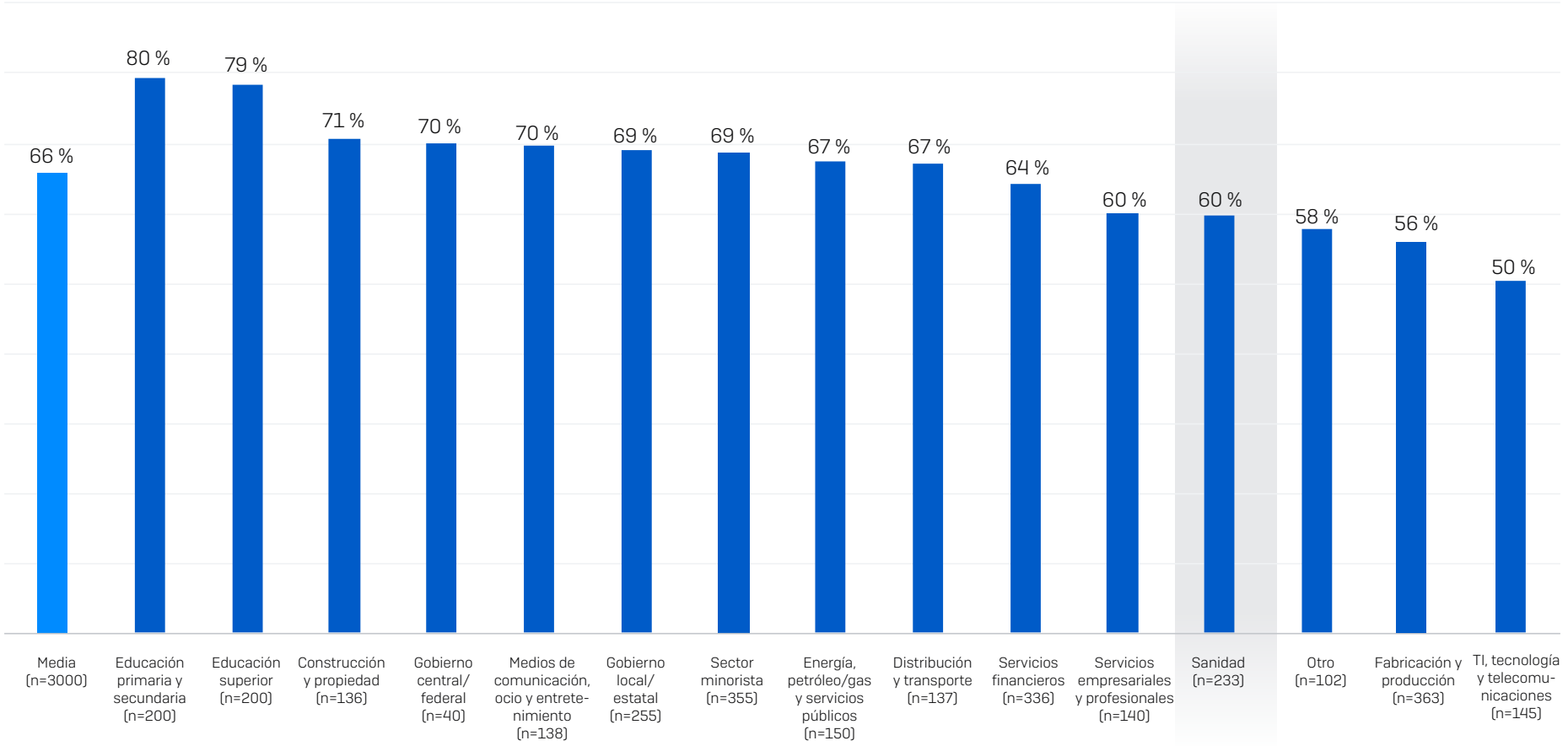
Las organizaciones deben centrarse en:

- 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).
- 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.
- 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

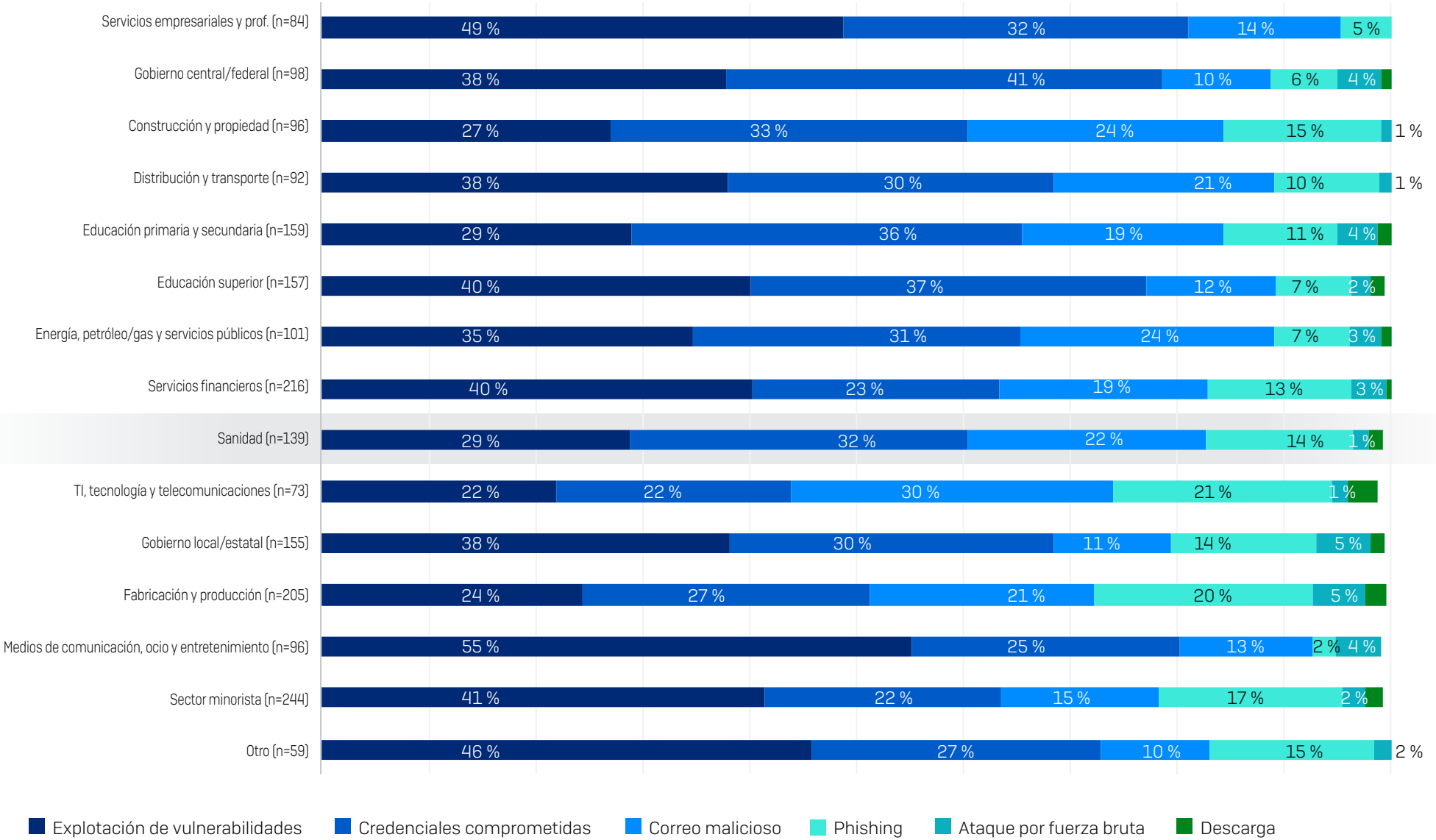
Ataques de ransomware por sector

Porcentaje de organizaciones atacadas por ransomware



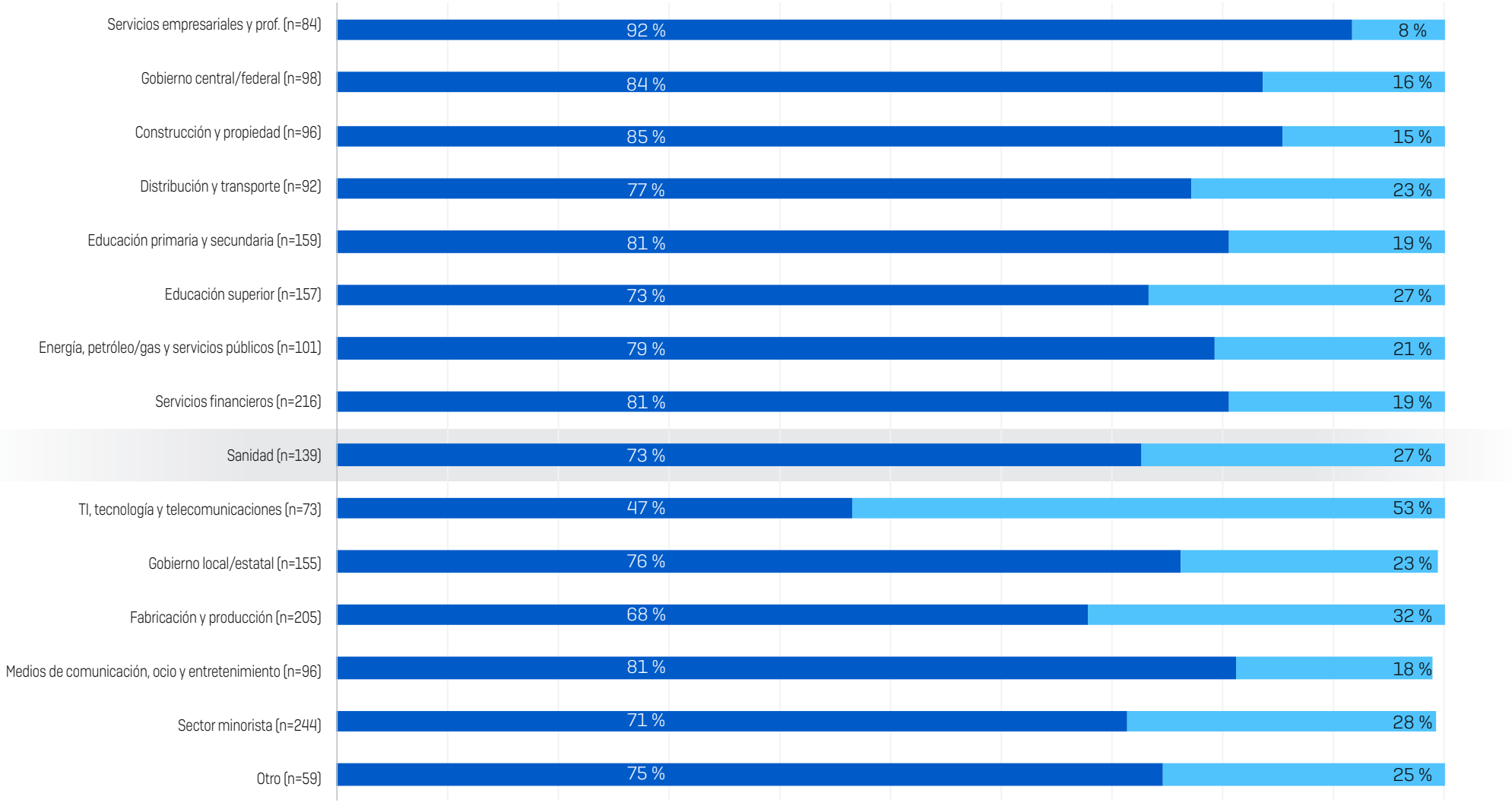
En el último año, ¿se ha visto afectada su organización por el ransomware? Números base en la tabla

Causas raíz del ataque por sector



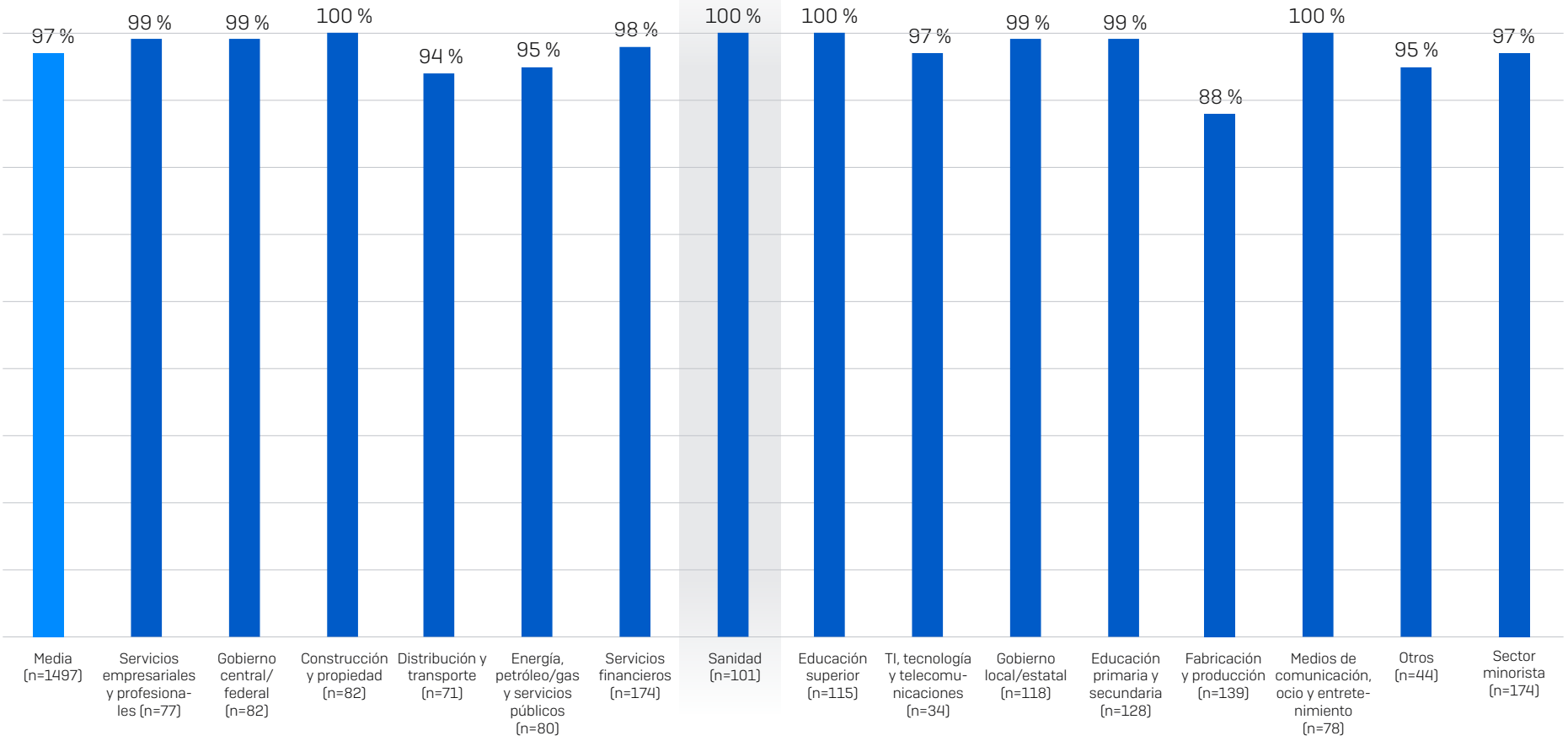
¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? Selección de opciones de respuesta. Números base en la tabla

Cifrado de datos por sector



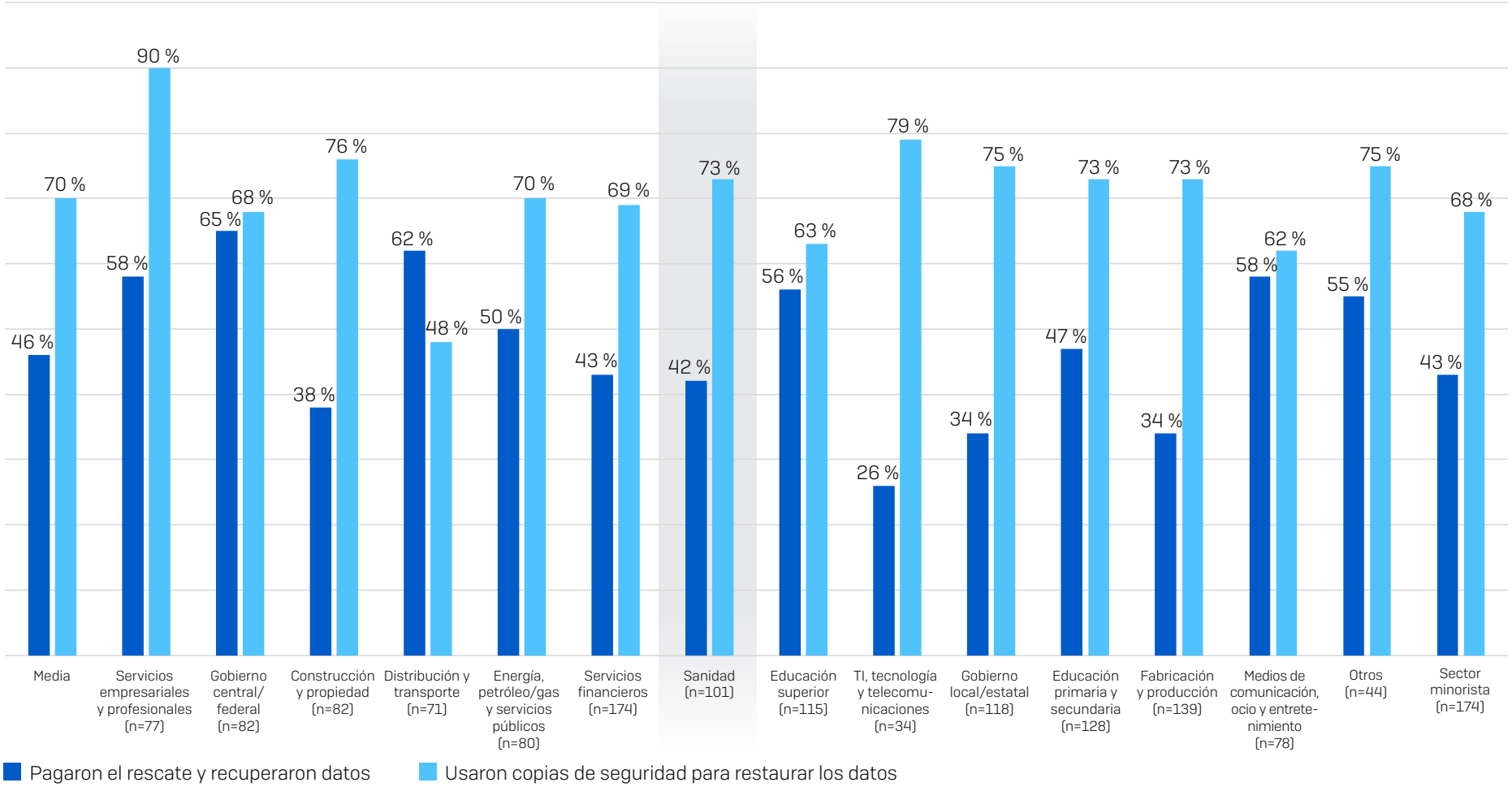
¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Consolidación de opciones de respuesta. Números base en la tabla

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

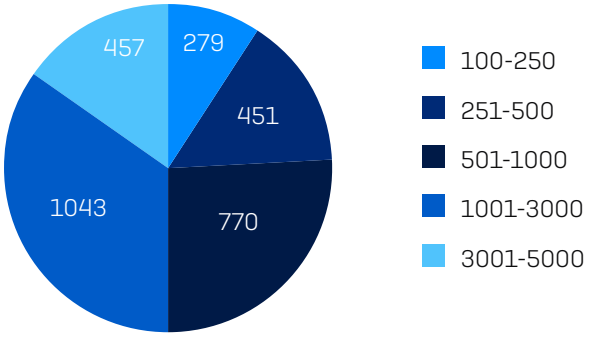
Sophos encargó una encuesta independiente y desvinculada de cualquier proveedor a 3000 responsables de TI/ciberseguridad y se realizó entre enero y marzo de 2023. Los encuestados provenían de 14 países repartidos por América, EMEA y Asia-Pacífico.

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.

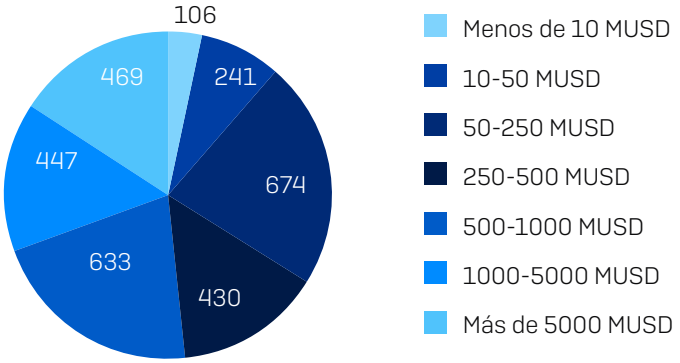
Encuestados por país

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.

2023-08-03 (WP-NP)

SOPHOS