SOPHOS

El estado del ransomware 2023

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

Monográficos de Sophos. Mayo 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 en 2023. Revela las causas raíz más comunes de los ataques y arroja nueva luz sobre cómo las experiencias con el ransomware difieren en función de los ingresos de la organización. 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 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.

Dentro del sector educativo, los encuestados se dividieron en educación primaria y secundaria (comprendiendo a los estudiantes hasta 18 años) y educación superior (estudiantes a partir de 18 años).

Contenido

Índice de los ataques de ransomware

El estudio reveló que el índice de ataques de ransomware se ha mantenido en el mismo nivel: un 66 % de los encuestados indicaron que sus organizaciones fueron víctimas de ataques de ransomware en el año anterior, igual que en nuestra encuesta de 2022. Viendo que los adversarios ahora son capaces de ejecutar sistemáticamente ataques a escala, podría decirse que el ransomware es el mayor ciberriesgo al que se enfrentan las organizaciones 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 un ataque. Para más información sobre el ransomware como servicio, lea el Informe de Sophos sobre amenazas 2023.

2020	2021	2022	2023
51 %	37 %	66 %	66 %

En el último año, ¿su organización ha sido víctima del ransomware?
Sí. n=3000 (2023), 5600 (2022), 5400 (2021), 5000 (2020)

Ataques por país

Mientras que el índice de ransomware general registrado se mantiene estable comparado con 2022, la encuesta reveló variaciones a nivel de país. Singapur registró el índice más alto de ataques de ransomware en el estudio de este año: un 84 % de las organizaciones se vieron atacadas en el último año. En cambio, el Reino Unido registró el índice más bajo de ataques (44 %).

Austria registró la mayor caída en el índice de ataques, pasando del 84 % de las organizaciones afectadas al 50 %. Sudáfrica experimentó el mayor aumento en el índice de ataques: el 78 % de las organizaciones se vieron afectadas en la encuesta de 2023, comparado con el 51 % en 2022.

Para más detalles, consulte el índice de ataques de ransomware por país: 2022 frente a 2023 en la página 20.

Ataques por sector

El sector educativo fue el más propenso a sufrir un ataque de ransomware en el último año: el 80 % de las escuelas primarias y secundarias y el 79 % de las instituciones de educación superior afirmaron haberse visto afectadas. Tradicionalmente, la educación tiene que lidiar con niveles de recursos y tecnología más bajos que muchos otros sectores, y los datos demuestran que los adversarios son conocedores de estas debilidades y las aprovechan.

El sector de TI, tecnología y telecomunicaciones registró el nivel más bajo de ataques (50 %), lo que indica un nivel más alto de ciberpreparación y ciberdefensas.

Para más detalles, consulte el índice de los ataques de ransomware por sector en la página 21.

66 % han sufrido un ataque de ransomware

Singapur: el índice más alto de ataques (país)

Reino Unido: el nivel más bajo de ataques (país)

Educación: el nivel más alto de ataques (sector)

TI, tecnología y telecomunicaciones:
el nivel más bajo de ataques (sector)

Ataques según el tamaño de la organización: Empleados frente a ingresos

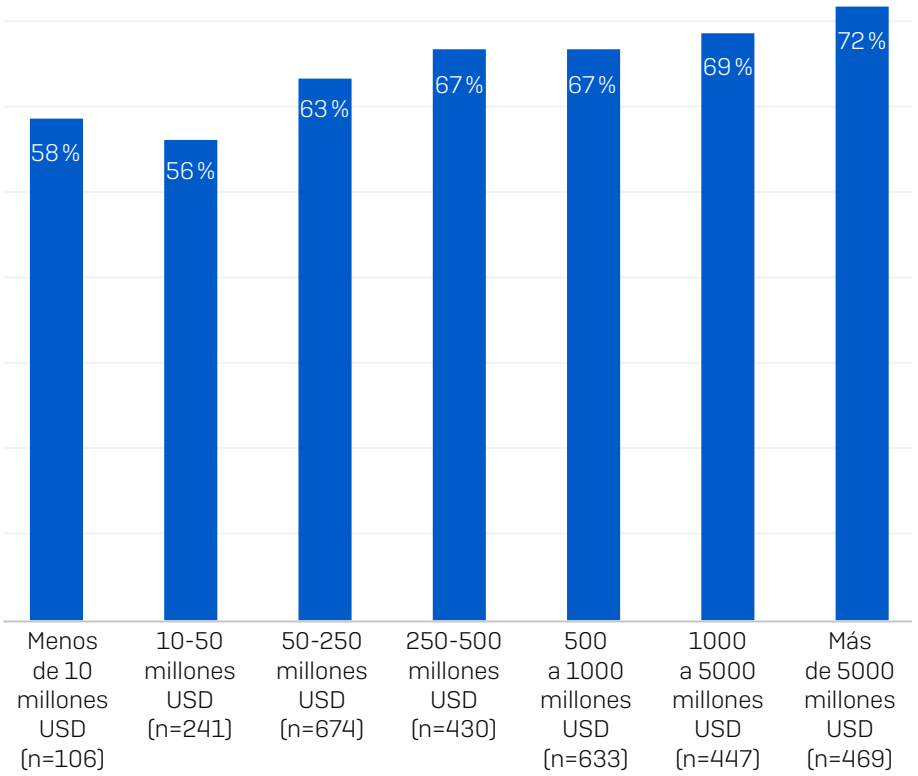
El estudio reveló una correlación clara entre los ingresos anuales y la propensión a ser el blanco de un ataque de ransomware, puesto que el porcentaje de organizaciones afectadas por el ransomware aumentaba progresivamente con los ingresos. El 56 % de las organizaciones con ingresos de entre 10 y 50 millones USD sufrió un ataque de ransomware en el último año, llegando al 72 % en aquellas empresas con ingresos de más de 5000 millones USD.

En cambio, no se observó una relación clara entre sufrir un ataque de ransomware y el número de empleados en una organización. Fuera del segmento de 1001-3000 empleados, el índice de los ataques de ransomware fue muy constante:

- 100-250 empleados 62 %
- 251-500 empleados 62 %
- 501-1000 empleados 62 %
- 1001-3000 empleados 73 %
- 3001-5000 empleados 63 %

Los datos ponen de manifiesto que, en el contexto del tamaño de la organización, los ingresos anuales son un indicador mucho más relevante en cuanto a la probabilidad de sufrir un ataque que el número de empleados.

Porcentaje de organizaciones atacadas por ransomware según los ingresos



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

Causas raíz de los ataques de ransomware

Según los encuestados, la causa raíz más común de los ataques de ransomware fue la explotación de una vulnerabilidad (36 %), seguida del compromiso de credenciales (29 %). Estos hallazgos coinciden casi exactamente con las conclusiones del último análisis retrospectivo de Sophos de 152 ataques en los que nuestros equipos de respuesta a incidentes y detección y respuesta gestionadas (MDR) tuvieron que intervenir. En él se detalla que el 37 % había empezado con la explotación de una vulnerabilidad y el 30 % con el compromiso de credenciales.

Los correos electrónicos fueron la causa raíz del 30 % (redondeando) de los ataques: El 18 % empezó con un correo malicioso y el 13 % con phishing. El 3 % comenzó con un ataque por fuerza bruta y solo un 1 % con una descarga.

¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? Si fue atacado más de una vez, piense en el ataque más significativo. (n=1974 organizaciones afectadas por el ransomware en el último año)

Causas raíz por sector

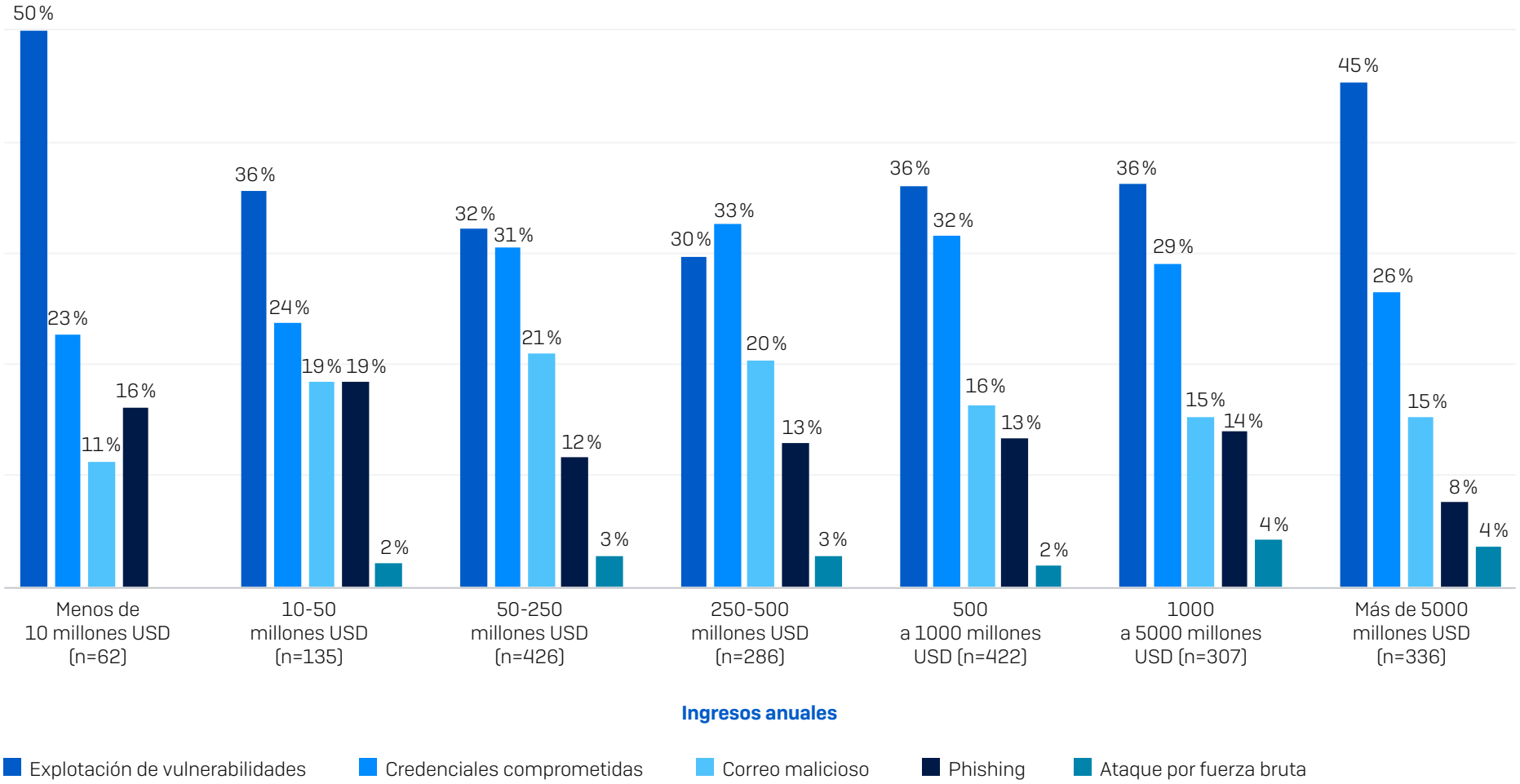
El sector de medios de comunicación, ocio y entretenimiento registró el porcentaje más alto de ataques cuya causa principal fue la explotación de una vulnerabilidad (55 %), lo que indica carencias de seguridad generalizadas en esta área. El gobierno central y federal registró el mayor porcentaje de ataques que empezaron con credenciales comprometidas (41 %). Esto puede ser debido a un mayor índice del robo de credenciales en este sector, a una capacidad menor para evitar la explotación de credenciales robadas o a una combinación de ambos.

El sector de TI, tecnología y telecomunicaciones presenta los índices más bajos en ambos casos: explotación de vulnerabilidades (22 %) y credenciales comprometidas (22 %), lo que probablemente refleja los altos niveles de ciberdefensas en este sector. Sin embargo, sí que registró las cifras más altas en ataques basados en el correo electrónico, ya que más de la mitad (51 %) se iniciaron en la bandeja de entrada de los usuarios.

Para más detalles, consulte las causas raíz de los ataques por sector en la página 22.

Causas raíz por ingresos

El análisis de las causas raíz en función de los ingresos anuales revela que la explotación de vulnerabilidades y el compromiso de credenciales siguen curvas de tendencia opuestas. Los porcentajes más altos de ataques que se iniciaron con la explotación de una vulnerabilidad corresponden a los grupos de organizaciones con los ingresos más bajos (menos de 10 millones USD: 50 %) y más altos (más de 5000 millones USD: 45 %), reduciéndose hasta el 30 % en el grupo intermedio (entre 250 y 500 millones USD). En cambio, el uso de credenciales comprometidas alcanza el pico en el grupo de ingresos intermedio (33 %), mientras que el uso más bajo corresponde a los grupos de ingresos más bajos (23 %) y más altos (26 %).

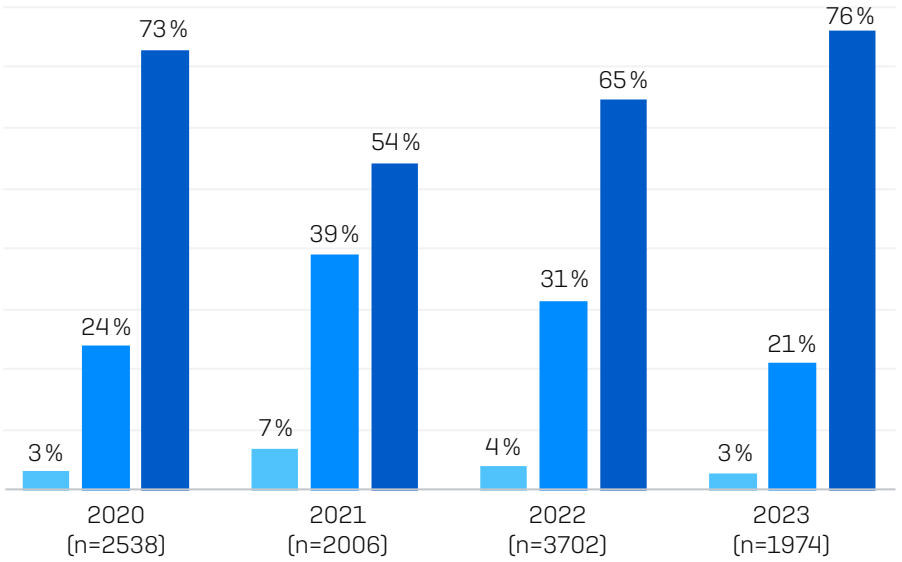


¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? Selección de opciones de respuesta. Números base en la tabla

Índice del cifrado de datos

El cifrado de datos continuó aumentando, y los adversarios consiguieron cifrar los datos en más de tres cuartas partes (76 %) de los ataques de ransomware. De hecho, los niveles de cifrado se sitúan ahora en su punto más alto de los últimos cuatro años. Esto probablemente refleja el nivel de habilidades cada vez mayor de los adversarios, que continúan innovando y perfeccionando sus métodos.

¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware?



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

Cifrado de datos por sector

Casi todos los sectores luchan por detener los ataques antes de que se produzca el cifrado de datos: con solo una excepción, en cada sector, más de dos tercios de los ataques comportaron el cifrado de datos. La máxima frecuencia del cifrado de datos (92 %) fue registrada por los servicios empresariales y profesionales.

El sector de TI, tecnología y telecomunicaciones es el que rompe la tendencia, puesto que los adversarios consiguieron cifrar los datos en menos de la mitad (47 %) de los ataques. Este es otro indicador del alto nivel de ciberdefensas y de preparación para responder a incidentes por el que se caracteriza este sector.

Para más detalles, consulte el cifrado de datos por sector en la página 23.

Robo de datos

En el 30 % de los ataques en que se cifraron 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.

30 %
ataques de ransomware en que se cifraron datos y también se robaron datos

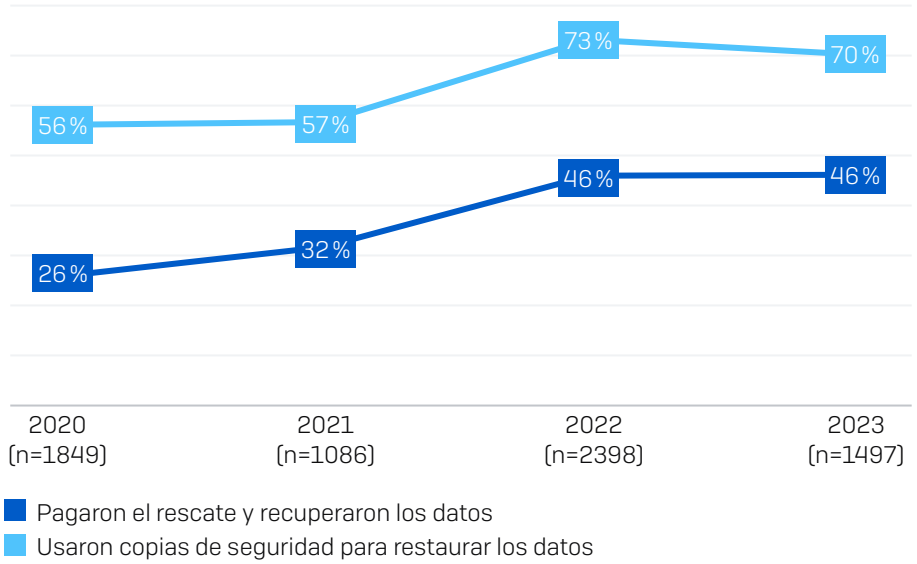
¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Sí; Sí, y los datos también fueron robados. n=1497

Recuperación de datos

El 97 % de las organizaciones cuyos datos fueron cifrados los recuperaron. Las copias de seguridad fueron el enfoque más común, y se utilizaron en el 70 % de los incidentes. El 46 % pagó el rescate y recuperó los datos, mientras que el 2 % empleó otros medios. En general, uno de cada cinco (21 %) utilizó varios métodos para restaurar sus datos. El 1 % de las organizaciones cuyos datos fueron cifrados pagaron el rescate pero no pudieron recuperar los datos.

Usaron copias de seguridad para restaurar datos	Pagaron el rescate y recuperaron los datos	Usaron otros medios para recuperar datos
70 %	**46 %**	**2 %**

Resulta preocupante que el uso de copias de seguridad para recuperar los datos haya disminuido con respecto al año anterior, cuando se utilizó en el 73 % de los casos. El índice de pago de rescates se ha mantenido en el mismo nivel del año anterior.



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

Recuperación de datos por país

En general, los encuestados de la región EMEA registraron en conjunto mayores niveles de uso de copias de seguridad (75 %) y menores niveles de pago de rescate (40 %) que los de América (65 %/55 %) y Asia-Pacífico (67 %/49 %). A nivel de país, Francia es el que más usa las copias de seguridad (87 %), seguido de cerca por Suiza (84 %).

La importancia de las copias de seguridad se demuestra cuando vemos que los dos países menos propensos a usar las copias de seguridad para restaurar datos, Italia (55 %) y Singapur (57 %), son también los dos países con los índices de recuperación de datos generales más bajos (93 % y 90 %, respectivamente). Italia es también el país más propenso a pagar el rescate (56 %), seguido de cerca por EE. UU. y Brasil (ambos 55 %).

En la mayoría de casos, las organizaciones que pagaron el rescate pudieron recuperar los datos. Sin embargo, en Francia y el Reino Unido, alrededor de una de cada diez organizaciones que pagaron el rescate no pudieron recuperar los datos.

Para más detalles, consulte la recuperación de datos por país en la página 24.

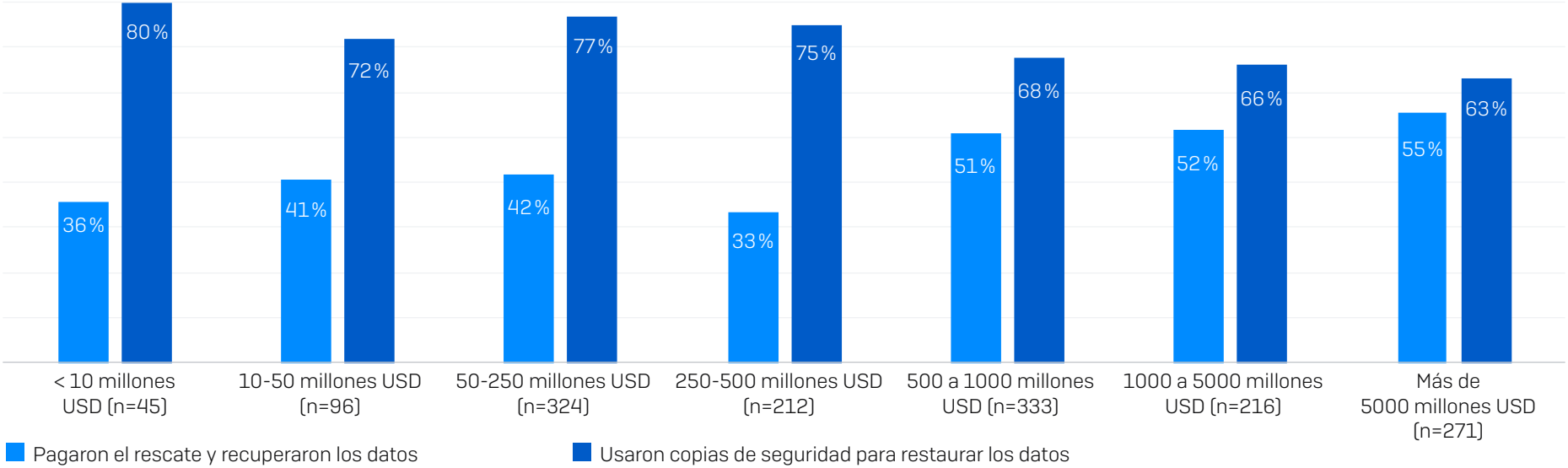
Pago de rescate y uso de copias de seguridad por ingresos

En general, a medida que los ingresos anuales aumentan, también crece la predisposición de una organización a recuperar los datos pagando el rescate. Al mismo tiempo, la frecuencia del uso de copias de seguridad disminuye.

De las organizaciones con ingresos por encima de los 5000 millones USD, el 55 % recuperó los datos pagando el rescate y el 63 % usó copias de seguridad. Al mismo tiempo, el 36 % de las organizaciones con ingresos inferiores a 10 millones USD recuperaron los datos pagando el rescate, mientras que el 80 % usó copias de seguridad: el índice más alto en el uso de copias de seguridad de todos los grupos de ingresos.

Las organizaciones con ingresos anuales más bajos tienen menos dinero para financiar el pago de rescates, lo que las obliga a centrarse en las copias de seguridad para la recuperación de datos. Paralelamente, las organizaciones con mayores ingresos suelen tener infraestructuras de TI complejas, hecho que puede dificultar usar copias de seguridad para recuperar los datos en un tiempo razonable. También son las empresas más propensas a pagar para salir de este tipo de situaciones.

Pago de rescate y uso de copias de seguridad por ingresos



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

El impacto de los ciberseguros en la recuperación de datos

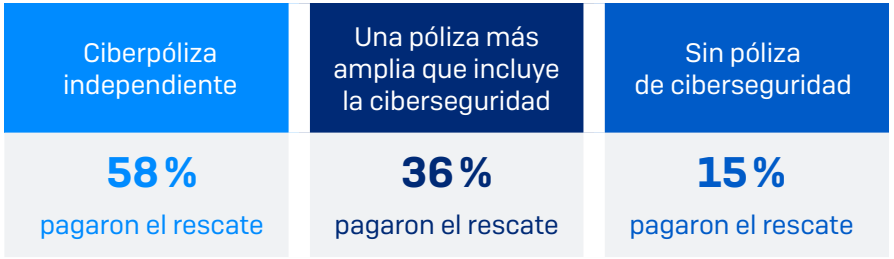
Las organizaciones con un ciberseguro contratado tenían muchas más probabilidades de recuperar los datos cifrados que aquellas sin este tipo de pólizas. Sin embargo, el tipo de cobertura en materia de ciberseguridad no supone una gran diferencia: el 98 % de las empresas con una ciberpóliza independiente y el 97 % de aquellas con una póliza más amplia con una cláusula de ciberseguridad pudieron recuperar los datos. En comparación, el 84 % de aquellas organizaciones sin una póliza pudieron recuperar sus datos cifrados.

Porcentaje de víctimas de ransomware que recuperaron sus datos cifrados

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

Probablemente hay varios factores que podrían explicar esta variación. Primero, los ciberseguros suelen requerir que las organizaciones tengan copias de seguridad y planes de recuperación como requisito para obtener cobertura. Las aseguradoras también pueden guiar a las víctimas del ransomware a través del proceso de recuperación para optimizar los resultados. Además, es más probable que las organizaciones con un ciberseguro paguen el rescate para recuperar los datos que aquellas sin una póliza.

Impacto del seguro en la propensión a pagar el rescate



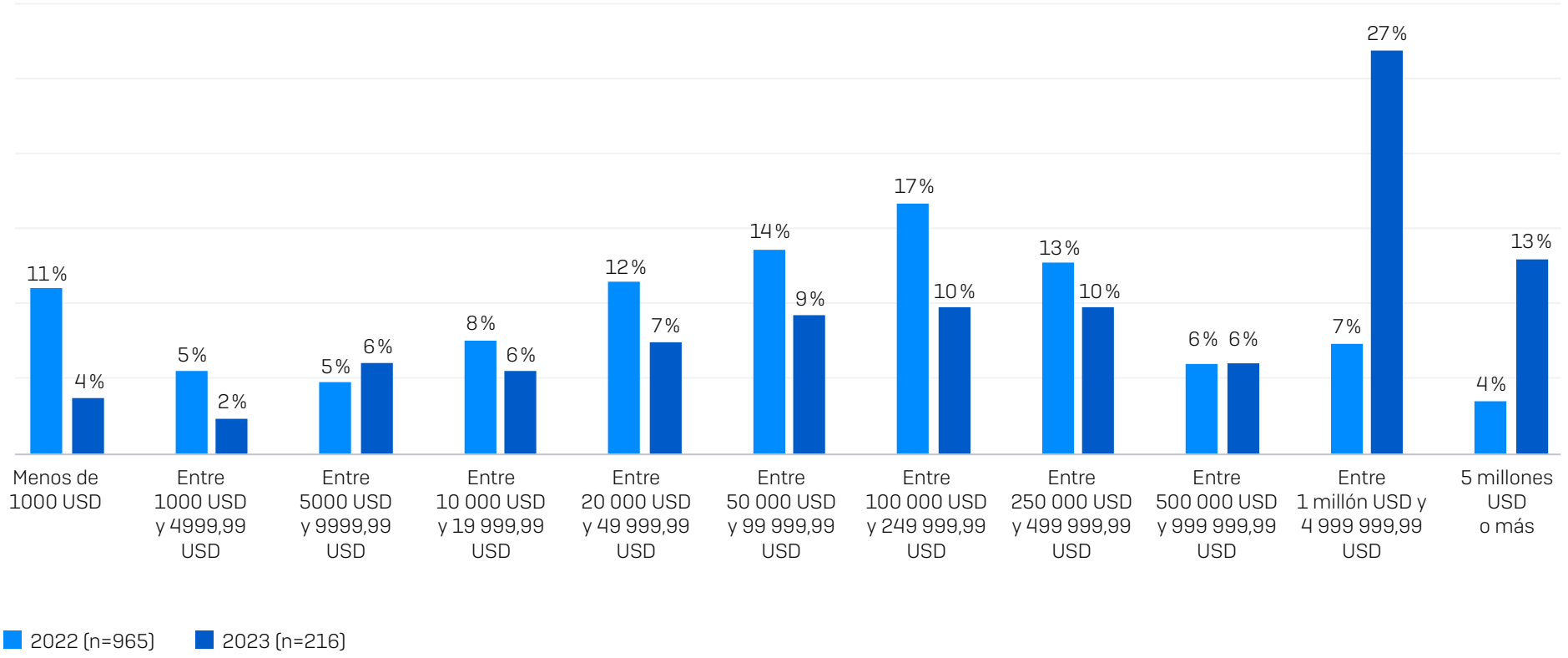
¿Recuperó su organización los datos? Sí, pagamos el rescate y recuperamos los datos. n=1497 organizaciones afectadas por el ransomware en el último año y cuyos datos fueron cifrados (771 ciberpóliza independiente, 658 cláusula de ciberseguridad como parte de una póliza más amplia, 67 sin póliza de ciberseguridad)

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 durante el último año: el importe de rescate medio casi se ha duplicado, pasando de 812 380 USD en 2022 a 1 542 333 USD en 2023. La mediana del pago de rescates según el estudio de este año es de 400 000 USD.

El estudio reveló una amplia distribución de los pagos, aunque la proporción de organizaciones que pagaron rescates más altos ha aumentado en comparación con nuestro estudio de 2022: un 40 % notificaron pagos de 1 millón USD o más, en comparación con el 11 % del año anterior. En cambio, solo un 34 % pagó menos de 100 000 USD, una disminución comparado con el 54 % del año anterior.

Pagos de rescate: 2023 frente a 2022



¿Cuál fue el importe del rescate que pagó su organización a los atacantes? Se excluyen las respuestas «No lo sé».

Pagos de rescate por ingresos

Quizás no es de extrañar que las organizaciones con mayores ingresos pudieran pagar rescates más altos. Esto refleja que los adversarios ajustan el importe que exigen en función de la capacidad de pago de la víctima. El estudio no distingue entre los pagos financiados internamente y los pagos financiados por ciberaseguradoras.

Es interesante observar que había muy poca diferencia tanto en la media como en la mediana de los pagos de rescates para las organizaciones con ingresos de entre 250 y 500 millones USD y aquellas con ingresos de entre 500 y 1000 millones USD.

	50-250 MILLONES USD (N=37)	250-500 MILLONES USD (N=33)	500 A 1000 MILLONES USD (N=72)	1000 A 5000 MILLONES USD (N=45)	MÁS DE 5000 MILLONES USD (N=21)
Importe medio del rescate	690996 $	1523652 $	1466240 $	2049817 $	2464339 $
Mediana del pago de rescate	145000 $	428000 $	425000 $	1000000 $	3000000 $

¿Cuál fue el importe del rescate que pagó su organización a los atacantes? Se excluyen las respuestas «No lo sé». Se excluyen las organizaciones con ingresos por debajo de 50 millones USD debido a números base muy bajos. Números base en la tabla. Los datos para segmentos con menos de 30 respuestas deben considerarse como meramente indicativos.

Costes de recuperación

El pago de rescates es solo un elemento de los costes de recuperación en la gestión de los eventos de ransomware. Si excluimos 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 y en línea con los 1,85 millones USD registrados en 2021.

Nota: el enunciado de la pregunta de los estudios de 2021 y 2022 incluía el importe del rescate pagado en los costes estimados, pero este importe se eliminó del enunciado en la encuesta de 2023. Como resultado, la comparación interanual debe considerarse meramente informativa.

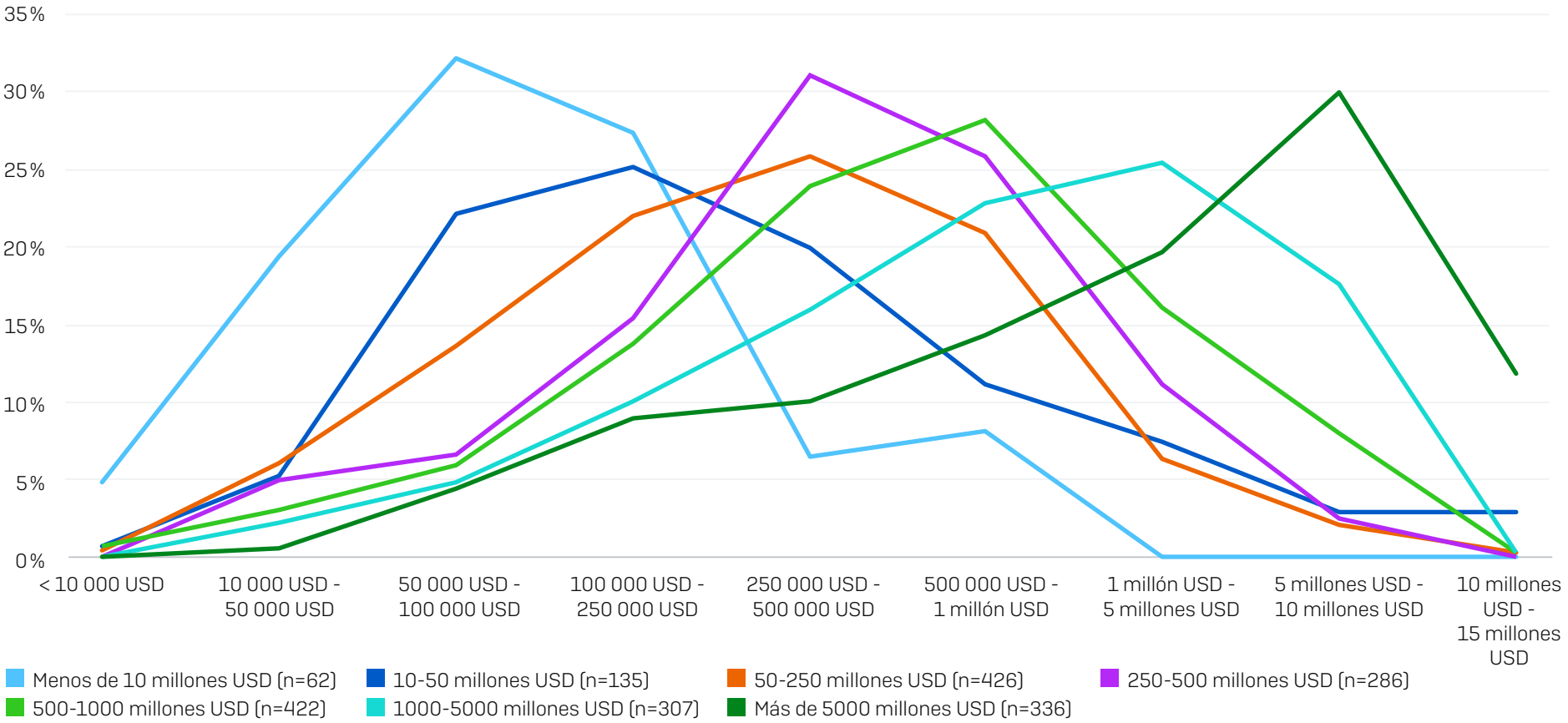
Coste de recuperación medio

2021	2022	2023
1,85 millones USD	1,4 millones USD	1,82 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.)? n=1974 (2023)/ 3702 (2022)/ 2006 (2021). Nota: el enunciado de la pregunta en las encuestas de 2022 y 2021 también incluía «pago de rescate».

Los costes de recuperación medios registrados se iniciaron en 165 520 USD para las organizaciones con ingresos anuales inferiores a 10 millones USD y subieron hasta 4 496 086 USD en el grupo de más de 5000 millones USD. Aunque estas cifras enmascaran distintos costes de recuperación, se ha observado un patrón claro de aumento de los costes de recuperación con los ingresos, tal y como se indica en el gráfico de la página siguiente.

Coste de recuperación por ingresos



¿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

Se mire como se mire, sale mucho más a cuenta usar copias de seguridad para recuperarse de un ataque de ransomware que pagar el rescate. 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 casi 1 millón USD menor para los que usaron copias de seguridad. Si se necesitaban más pruebas de las ventajas financieras de invertir en una estrategia sólida de copias de seguridad, aquí están.

Pagaron el rescate y recuperaron los datos	Usaron copias de seguridad para restaurar datos
750 000 USD mediana	**375 000 USD** mediana
2,6 millones USD promedio	**1,62 millones USD** promedio

¿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.)? n=694 que pagaron el rescate y recuperaron los datos y 1053 que usaron copias de seguridad para restaurar los datos.

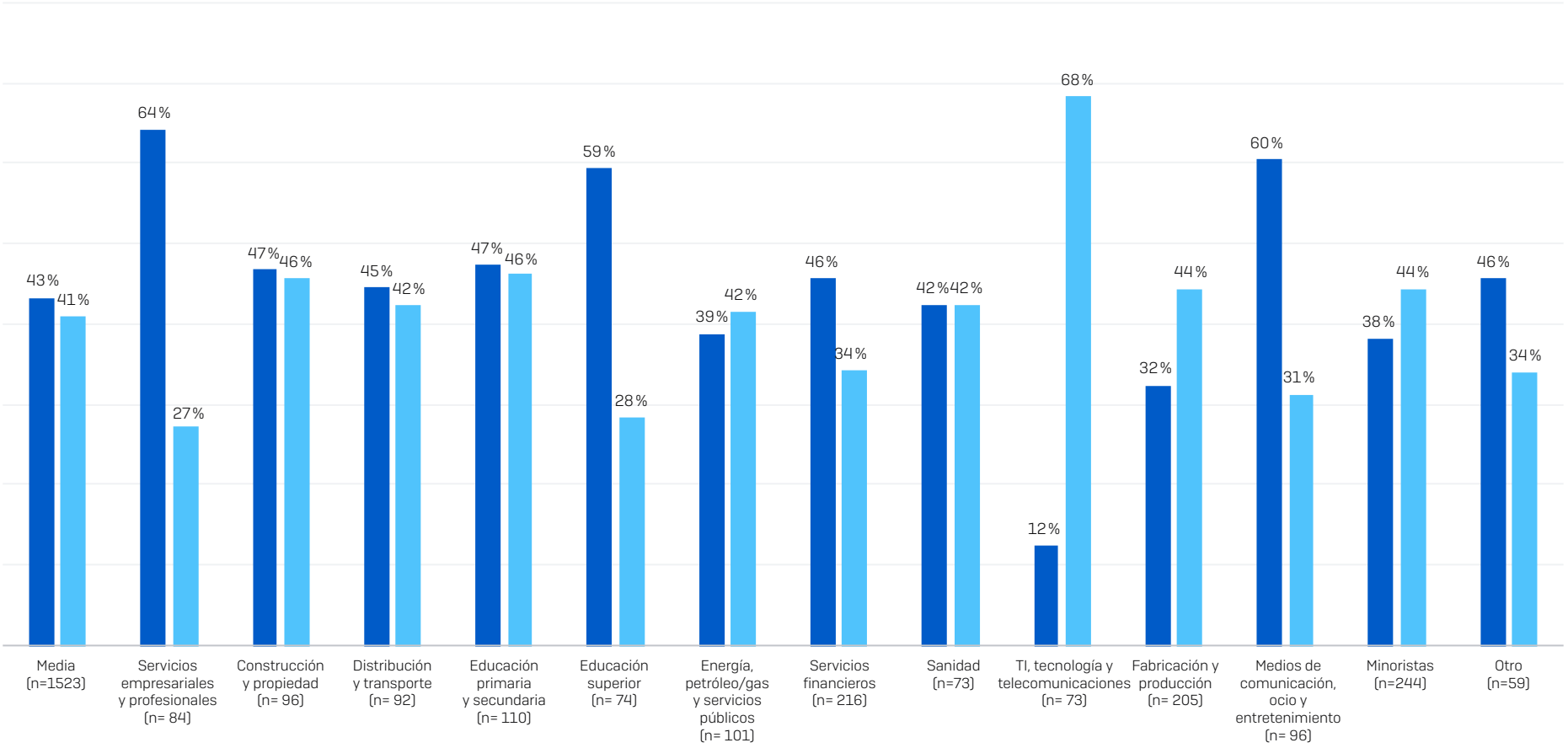
Impacto empresarial

El 84 % de las organizaciones del sector privado que se han visto afectadas por un ataque de ransomware señalaron que sufrieron pérdidas de negocio/ingresos. Los ingresos anuales influyeron relativamente poco en la pérdida de negocio. El índice más bajo (79 %) se registró en el grupo con una facturación de entre 250 y 500 millones USD, y el índice más alto (88 %) en aquellos con ingresos de menos de 10 millones USD y de más de 5000 millones USD.

El tipo de sector ha desempeñado un papel mucho más significativo en la propensión a sufrir pérdidas de negocio/ingresos. En general, la educación primaria y secundaria (94 %) y la construcción y propiedad (93 %) fueron los sectores más propensos a declarar una pérdida de negocio/ingresos debido a los ataques, mientras que el sector de la fabricación y producción fue el menos propenso (77 %).

Si profundizamos en esta cuestión, vemos una variación considerable en los sectores que afirmaron haber sufrido «grandes pérdidas» de negocio/ingresos: los servicios empresariales y profesionales (64 %) son cinco veces más propensos a sufrir un ataque si lo comparamos con el 12 % del sector de TI, tecnología y telecomunicaciones.

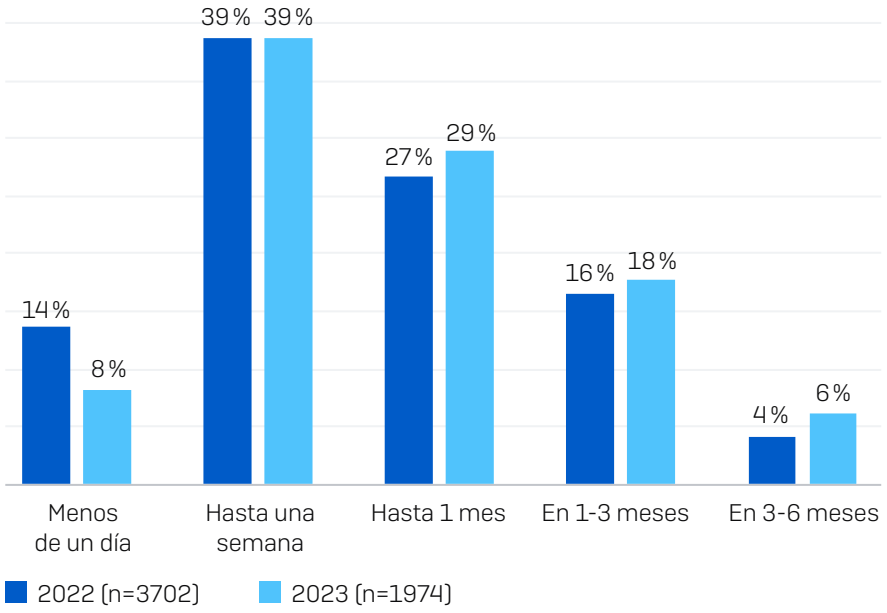
Pérdida de negocio/ingresos por sector



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

Tiempo de recuperación

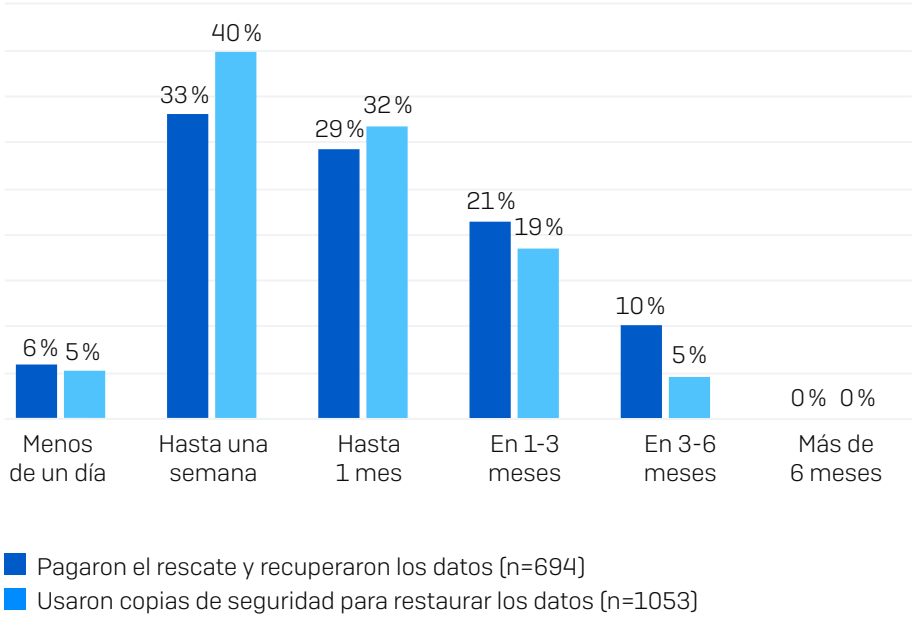
Mientras que el tiempo para recuperarse de un ataque de ransomware va en la misma línea que el informe de 2022, el porcentaje de los que pudieron recuperarse en menos de un día ha caído del 14 % al 8 %.



¿Cuánto tiempo necesitó su organización para recuperarse por completo del ataque de ransomware?
Números base en la tabla

Tiempo de recuperación por método de recuperación de datos

La investigación reveló que las organizaciones que usan copias de seguridad para recuperar sus datos se recuperan del ataque mucho más rápido que las que pagan el rescate. El 45 % de aquellas que usaron copias de seguridad se recuperaron en una semana, comparado con el 39 % de las que pagaron un rescate. Casi un tercio (32 %) de las que pagaron el rescate tardaron más de un mes en recuperarse, mientras que la cifra de las empresas que emplearon las copias de seguridad es del 23 % (redondeando). 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

Independientemente de los ingresos, la geografía o el sector, el ransomware continúa siendo una amenaza importante para las organizaciones. A medida que los adversarios continúan mejorando sus tácticas, técnicas y procedimientos de ataque (TTP), los responsables de la seguridad luchan por seguir el ritmo de los delincuentes, lo que resulta en mayores índices de cifrado.

La caída en el uso de copias de seguridad para recuperar datos cifrados es un motivo de preocupación importante. Si se necesitaban más pruebas de los beneficios financieros y operativos de invertir en una estrategia sólida de copias de seguridad, este informe las proporciona.

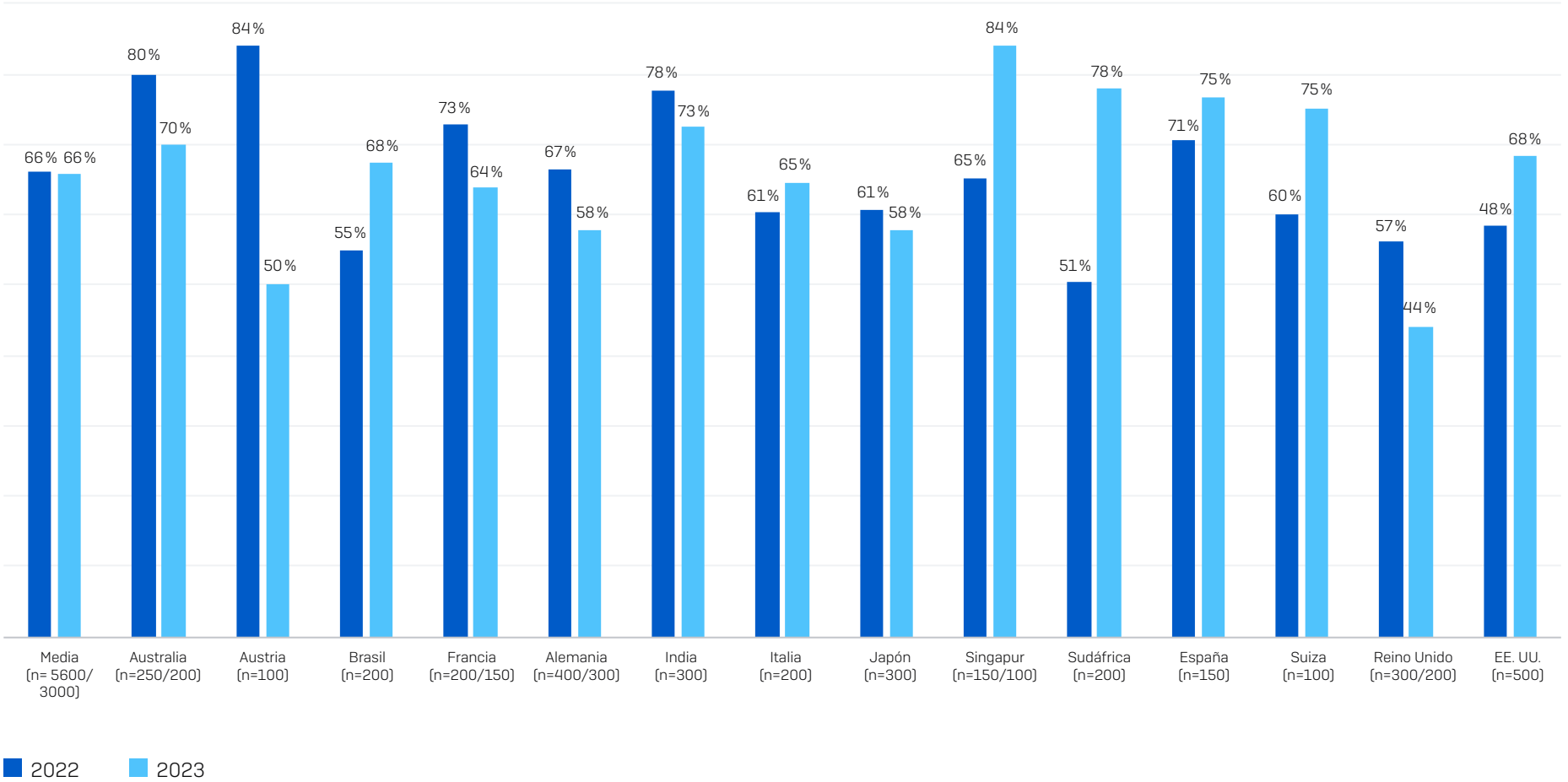
Con el crecimiento del modelo de negocio del ransomware como servicio, no prevemos un descenso de los ataques en el próximo año. Las organizaciones deben centrarse en:

- 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

Índice de los ataques de ransomware por país: 2022 frente a 2023

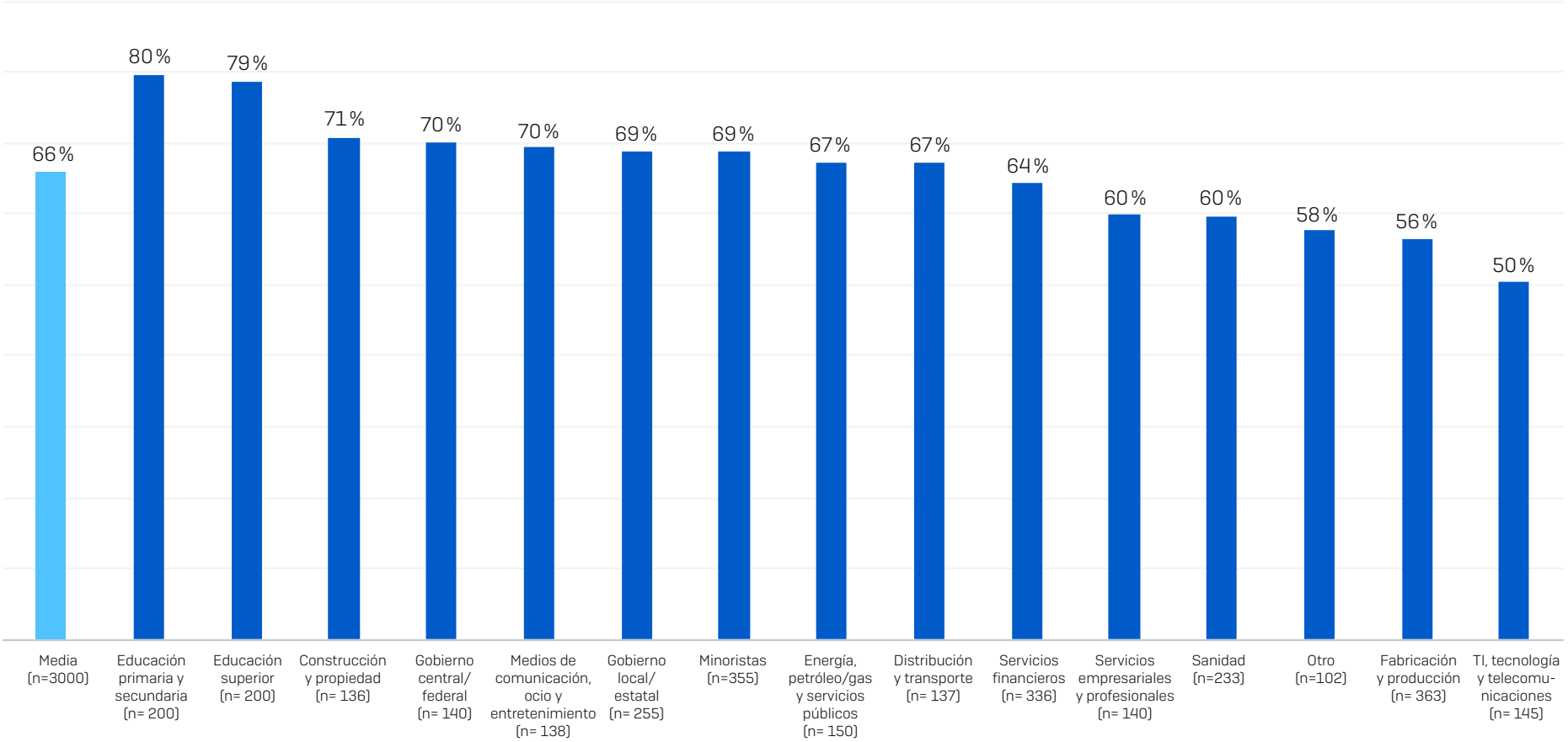
Porcentaje de organizaciones atacadas por ransomware



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

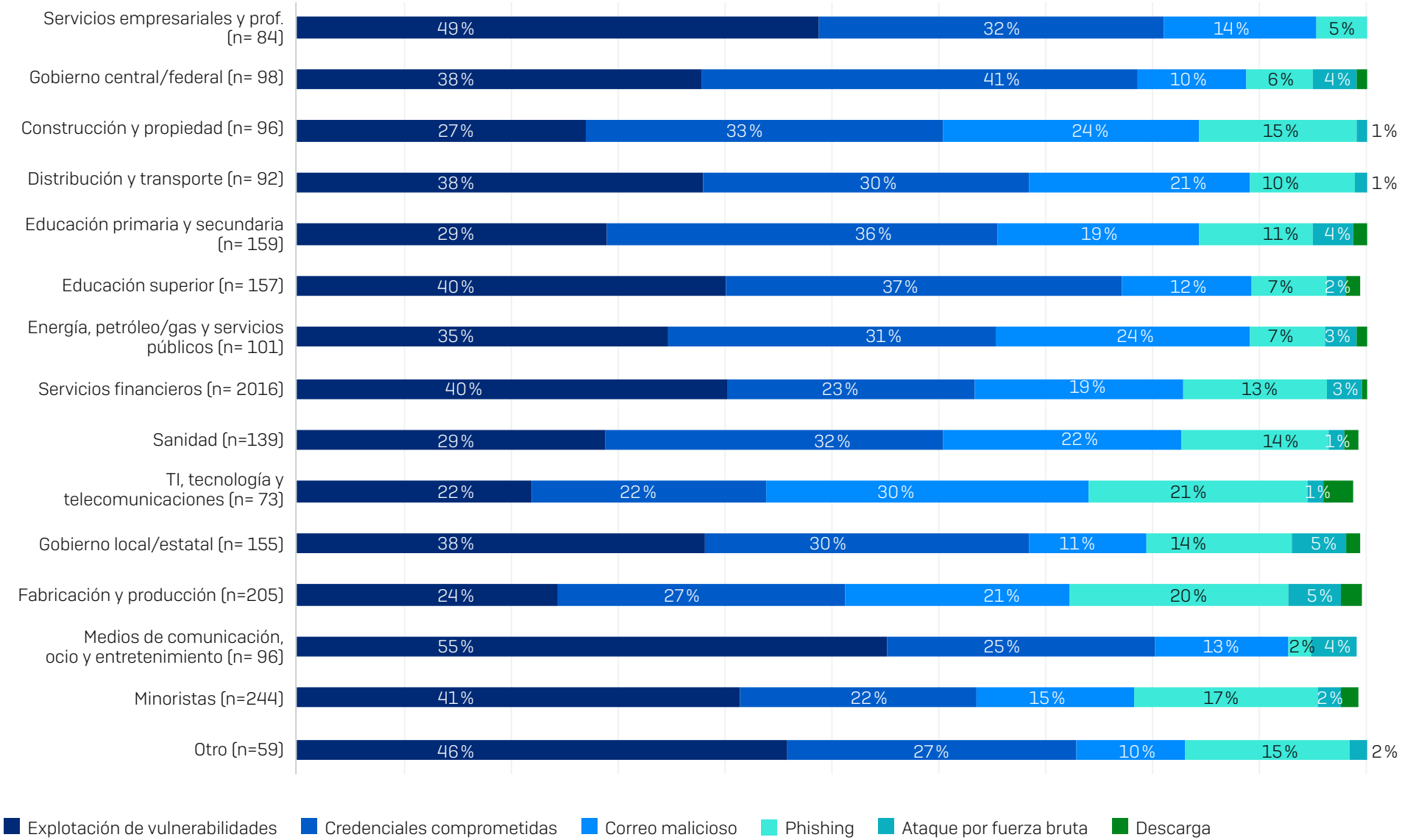
Índice de los ataques de ransomware por sector

Porcentaje de organizaciones atacadas por ransomware



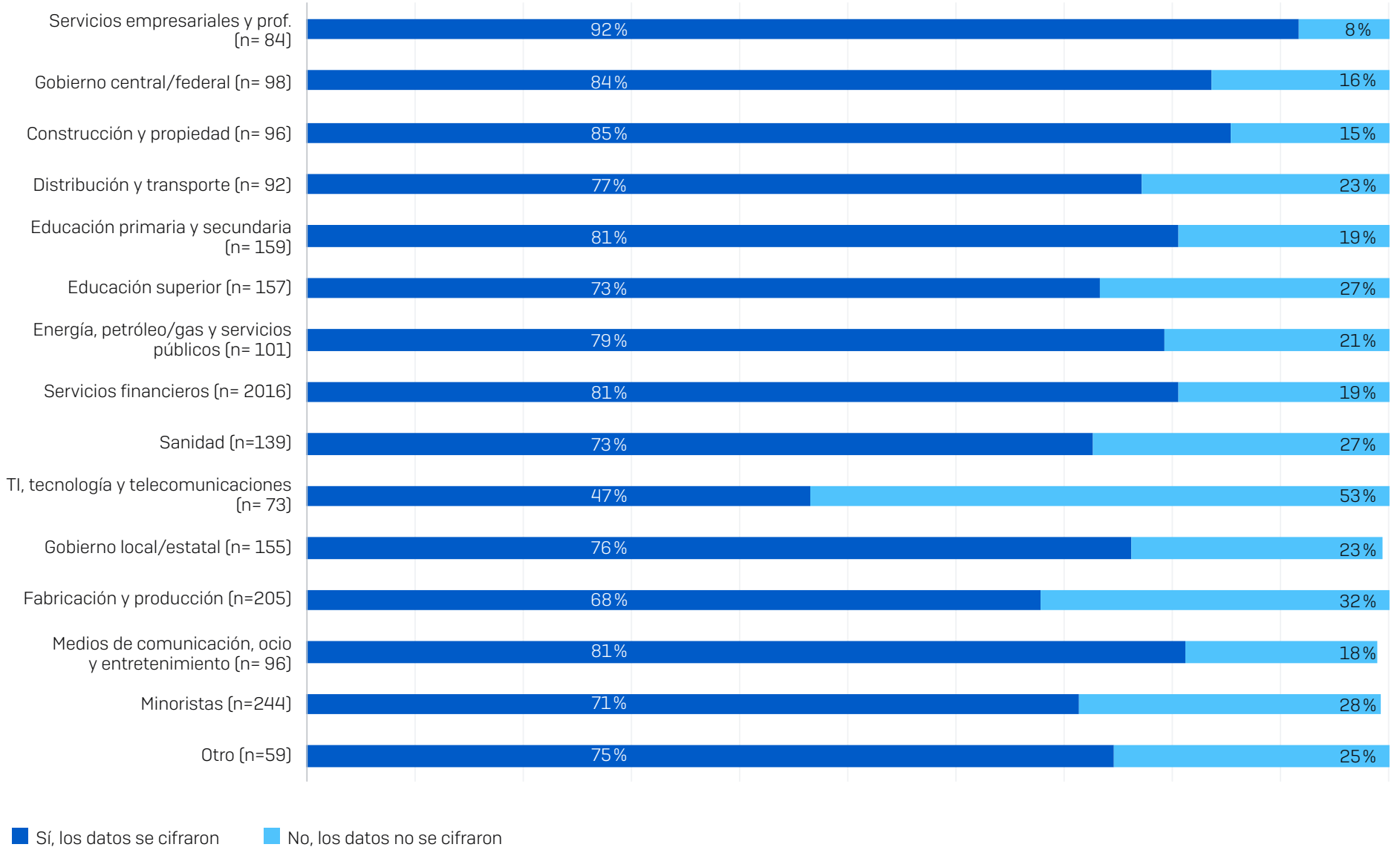
En el último año, ¿se ha visto afectada su organización por el ransomware? Números base en la tabla

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



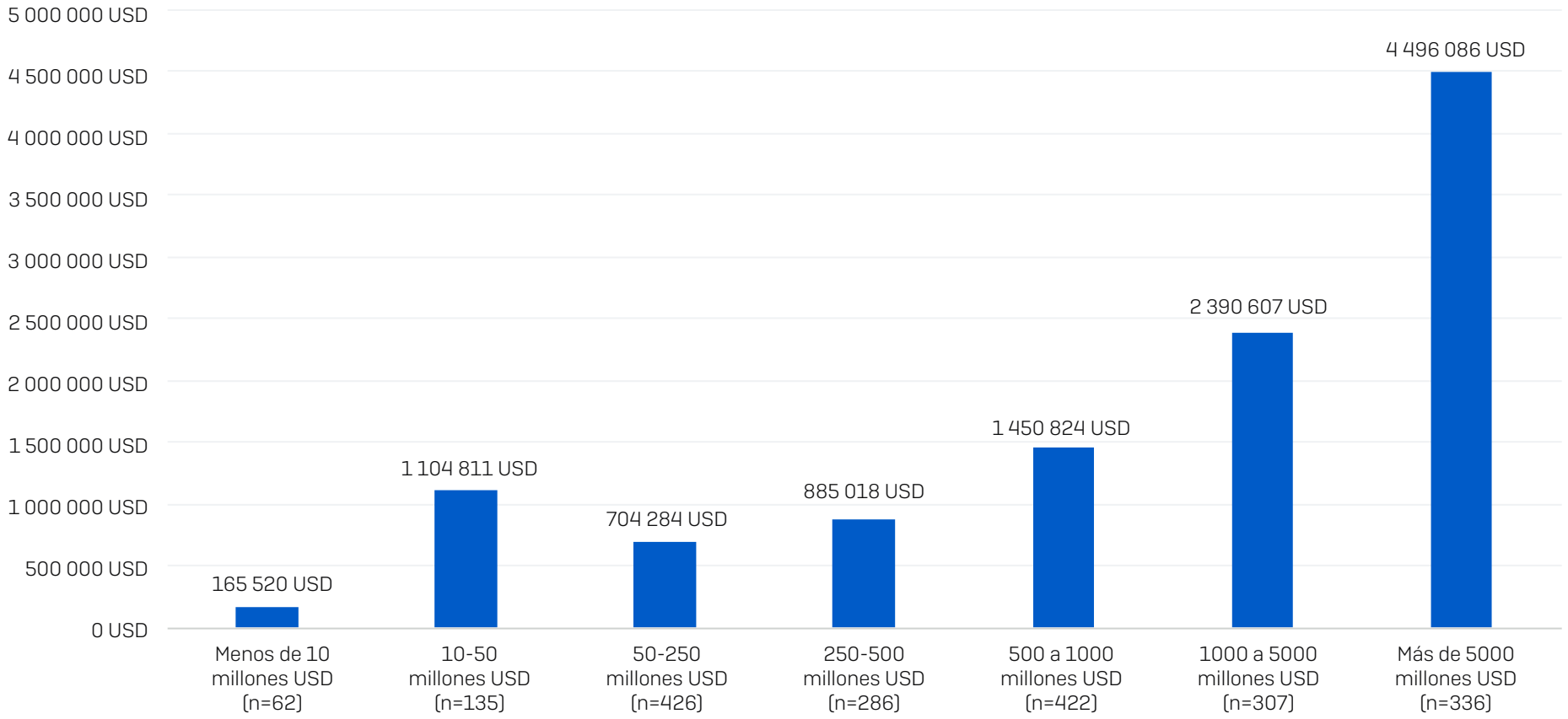
¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Consolidación de opciones de respuesta. Números base en la tabla

Recuperación de datos por país

¿Recuperó su organización los datos?

	EE. UU. (N=274)	BRASIL (N=98)	ALEMANIA (N=122)	AUSTRIA (N=48)	SUIZA (N=68)	REINO UNIDO (N=66)	ITALIA (N=82)	ESPAÑA (N=93)	FRANCIA (N=68)	SUDÁFRICA (N=139)	INDIA (N=167)	AUSTRALIA (N=96)	JAPÓN (N=125)	SINGAPUR (N=51)
Sí, pagamos el rescate y recuperamos los datos	54%	55%	44%	42%	38%	44%	54%	29%	22%	45%	43%	53%	52%	53%
Sí, usamos copias de seguridad para restaurar los datos	66%	61%	78%	73%	84%	68%	55%	81%	87%	76%	73%	73%	60%	57%
Sí, usamos otros medios para recuperar nuestros datos	1%	4%	1%	0%	3%	0%	0%	0%	3%	3%	3%	3%	6%	0%
No, aunque pagamos el rescate	1%	0%	0%	0%	0%	5%	2%	0%	3%	0%	1%	0%	0%	0%
No, no pagamos el rescate	0%	1%	2%	2%	1%	2%	5%	2%	0%	0%	1%	1%	5%	10%
No lo saben	0%	0%	2%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%
Recuperamos los datos mediante cualquier método	99%	99%	95%	98%	99%	94%	93%	98%	97%	100%	98%	99%	95%	90%
Utilizamos más de un método para recuperar los datos	22%	21%	27%	17%	26%	18%	16%	12%	12%	24%	20%	29%	22%	20%
Pagaron el rescate	55%	55%	44%	42%	38%	48%	56%	29%	25%	45%	44%	53%	52%	53%
Porcentaje de aquellos que pagaron el rescate pero no pudieron recuperar los datos	1%	0%	0%	0%	0%	9%	4%	0%	12%	0%	3%	0%	0%	0%

Coste medio de recuperación por ingresos



¿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.

Metodología de investigación

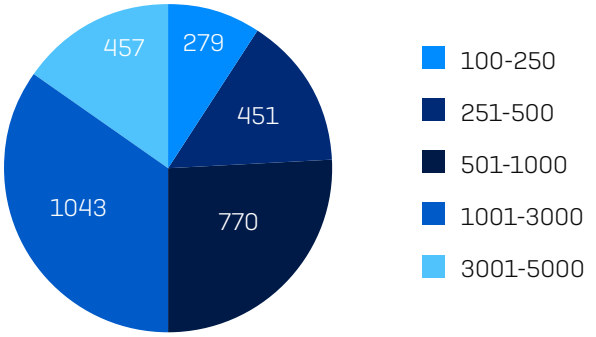
Sophos encargó una encuesta independiente y desvinculada de cualquier proveedor a 3000 responsables de TI/ciberseguridad y se realizó entre enero y marzo de 2023. Los encuestados provenían de 14 países repartidos por América, EMEA y Asia-Pacífico.

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.

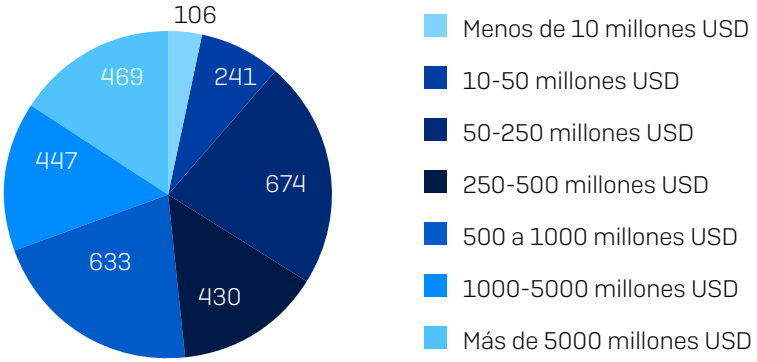
Encuestados por país

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.

2023-05-05 (WP-DD)

SOPHOS