SOPHOS

El estado del ransomware 2024

Resultados de una encuesta independiente y desvinculada de cualquier proveedor a 5000 responsables de TI/ciberseguridad en 14 países, realizada entre enero y febrero de 2024.

Monográficos de Sophos. Abril 2024

Introducción

El quinto estudio anual de Sophos sobre las experiencias reales con el ransomware de organizaciones de todo el mundo analiza el periplo de las víctimas, desde la causa raíz hasta la gravedad del ataque, el impacto financiero y el tiempo de recuperación. Los nuevos datos, combinados con las lecciones aprendidas de nuestros estudios anteriores, revelan las realidades a las que se enfrentan las empresas hoy en día, y también cómo ha evolucionado el impacto del ransomware en los últimos cinco años.

El informe de este año también incorpora nuevas secciones de estudio, incluido el análisis de las peticiones de rescate frente a los importes pagados, así como un mayor énfasis en el impacto que tienen los ingresos de una organización en el resultado de los ataques de ransomware. Además, por primera vez, arroja luz sobre el papel de las fuerzas del orden en la remediación del ransomware.

Nota sobre las fechas del informe

Para que resulte más fácil comparar los datos de nuestras encuestas anuales, damos al informe el nombre del año en que se ha realizado la encuesta, en este caso, 2024. Somos conscientes de que los encuestados comparten sus experiencias del año anterior, por lo que muchos de los ataques a los que se hace referencia se produjeron en 2023.

Acerca de la encuesta

Los resultados se basan en una encuesta independiente y desvinculada de cualquier proveedor encargada por Sophos a 5000 responsables de TI/ciberseguridad en 14 países de América, EMEA y Asia-Pacífico. Todos los encuestados representan a organizaciones de entre 100 y 5000 empleados. La encuesta fue realizada por la consultora Vanson Bourne entre enero y febrero de 2024, y se pidió a los participantes 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).

Índice de los ataques de ransomware

El año pasado, el 59 % de las organizaciones se vieron afectadas por el ransomware, un pequeño pero bienvenido descenso respecto al 66 % de los dos años anteriores. Aunque todo descenso es positivo, teniendo en cuenta que más de la mitad de las organizaciones han sufrido un ataque, no es momento de bajar la guardia.

2020	2021	2022	2023	2024
51 %	37 %	66 %	66 %	59 %

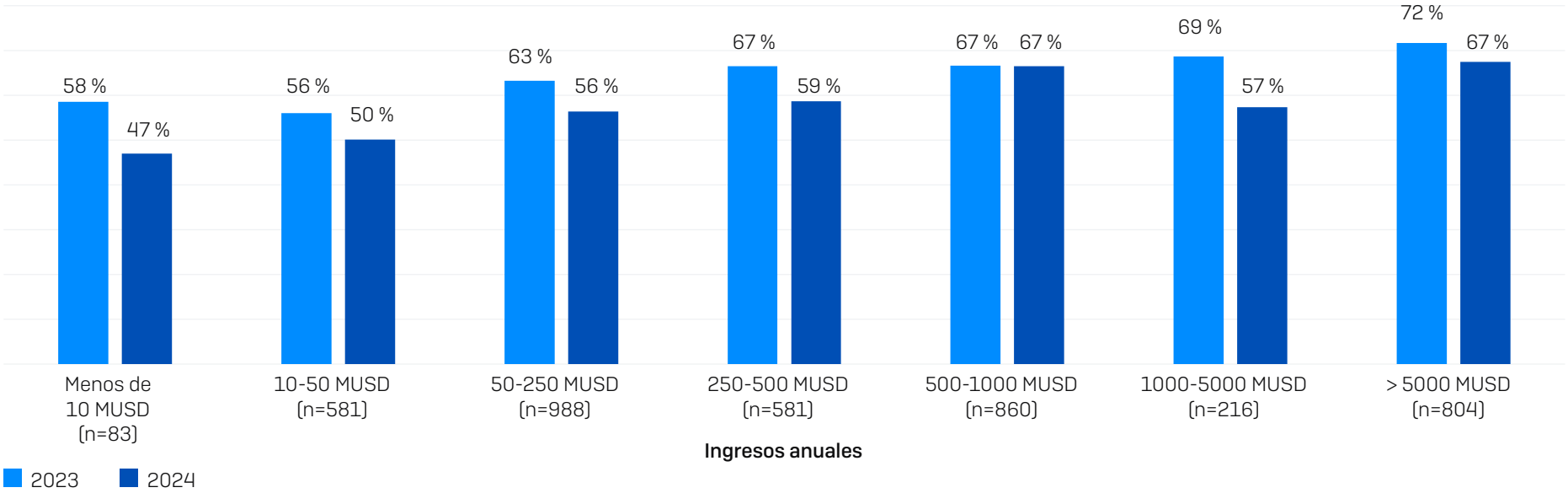
En el último año, ¿se ha visto afectada su organización por el ransomware?
Sí. n=5000 (2024), 3000 (2023), 5600 (2022), 5400 (2021), 5000 (2020).

Ataques por ingresos

Resulta alentador que todos los tramos de ingresos registraran una reducción del índice de ataques de ransomware en el último año (aunque en el caso de 500-1000 millones USD, fue inferior a un punto porcentual).

La predisposición a sufrir un ataque de ransomware suele aumentar con los ingresos, y las organizaciones de más de 5000 millones USD registran el índice más alto de ataques (67 %). Sin embargo, incluso las organizaciones más pequeñas (con unos ingresos inferiores a 10 millones USD) son víctimas frecuentes: algo menos de la mitad (47 %) sufrieron ataques de ransomware en el último año. Aunque muchos ataques de ransomware son perpetrados por bandas sofisticadas y bien financiadas, está aumentando el uso de ransomware básico y barato por parte de hackers mucho menos cualificados.

Porcentaje de organizaciones afectadas por el ransomware en el último año



En el último año, ¿se ha visto afectada su organización por el ransomware? Sí. n=5000 (2024), 3000 (2023). Números base de 2024, por tramo, en el gráfico.

Ataques por sector

Salvo algunas excepciones, los índices de ataques de ransomware fueron muy similares en los distintos sectores: afectaron a entre el 60 % y el 68 % de las organizaciones en 11 de los 15 sectores analizados. En el estudio de este año, los sectores que salen mejor parados son el del *gobierno estatal/local* (34 %) y el del *comercio minorista* (45 %), donde menos de la mitad de los encuestados afirmaron haber sido víctimas en el último año.

Curiosamente, los dos sectores gubernamentales ocupan posiciones opuestas: el *gobierno central/federal* ha registrado el mayor índice de ataques de todos los sectores (68 %), el doble que el *gobierno estatal/local* (34 %). Al mismo tiempo, en consonancia con la tendencia general a la baja de los ataques, el índice del *gobierno central/federal* es inferior a la cifra del sector en 2023, que fue del 70 %.

Hay varias razones que podrían explicar tal variación en el sector gubernamental. En un año de malestar generalizado, puede ser que los gobiernos centrales hayan experimentado un aumento de los ataques por motivos políticos. Los resultados también podrían obedecer a los esfuerzos realizados el año pasado por las organizaciones gubernamentales estatales/locales para reforzar su resiliencia ante los ataques, o a un cambio de estrategia de los adversarios en respuesta a la limitada capacidad del gobierno estatal/local para pagar rescates.

En el último año, se han producido otros cambios notables a nivel de sector:

- Se ha reducido el índice individual más alto de ataques registrado, que ha pasado del 80 % (*educación primaria y secundaria*) al 69 % (*gobierno central/federal*).
- El sector de la educación ya no presenta los dos índices de ataque más elevados: este año se sitúan en el 66 % (*educación superior*) y el 63 % (*educación primaria y secundaria*), frente al 79 % y al 80 %, respectivamente, del año pasado.
- El *sector sanitario* es uno de los cinco sectores que registraron un aumento del índice de ataques en el último año, pasando del 60 % al 67 %.
- El sector de *TI, telecomunicaciones y tecnología* ya no ostenta el índice de ataques más bajo: un 55 % de las organizaciones fueron víctimas en el último año, lo que supone un aumento con respecto al 50 % registrado en 2023.

Consulte el apéndice para ver un desglose detallado del índice de ataques de ransomware por sector.

Ataques por país

Francia registró el índice más alto de ataques de ransomware en 2024: un 74 % de los encuestados afirmaron haber sufrido un ataque en el último año, y la siguieron Sudáfrica (69 %) e Italia (68 %). En el extremo opuesto, los índices de ataque más bajos fueron los registrados por los encuestados de Brasil (44 %), Japón (51 %) y Australia (54 %).

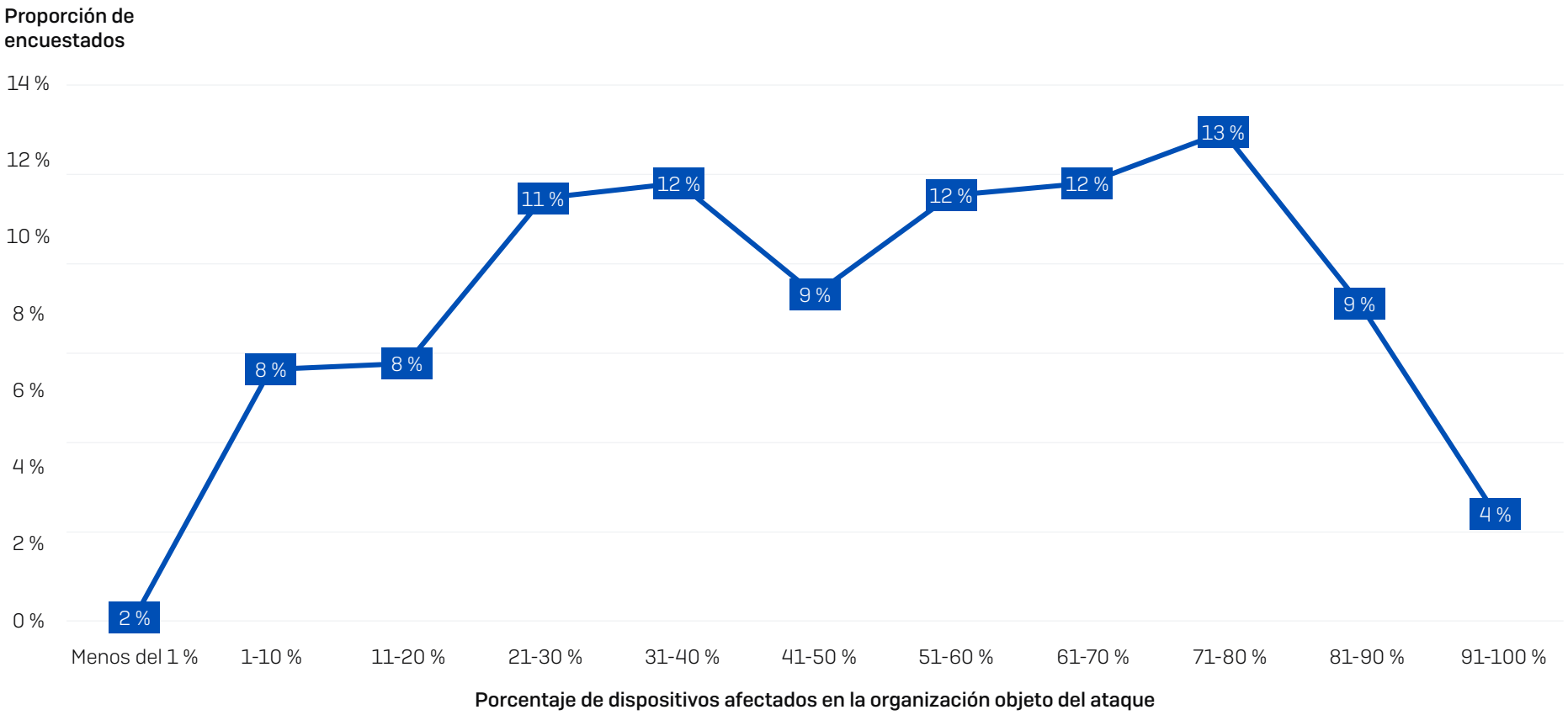
En términos generales, nueve países presentaron un índice de ataques inferior al de 2023. Los cinco países que registraron un índice de ataques superior al de 2023 están en Europa: Alemania, Austria, Francia, Italia y el Reino Unido (el aumento de Alemania fue inferior al 1 %). Esto puede deberse a un incremento de los ataques a organizaciones europeas o a que las defensas europeas no han podido seguir el ritmo de la evolución de los comportamientos de los atacantes como en otras zonas geográficas.

Consulte el apéndice para ver un desglose detallado del índice de ataques de ransomware por país.

Porcentaje de ordenadores afectados

De media, algo menos de la mitad (49 %) de los ordenadores de una organización se ven afectados por un ataque de ransomware. Sufrir el cifrado de todo el entorno es muy poco frecuente: solo el 4 % de las organizaciones señalaron que el 91 % o más de sus dispositivos habían sido alcanzados por un ataque. En el extremo opuesto, si bien algunos ataques afectan solo a un puñado de dispositivos, esto también es muy poco habitual. Según el informe, solo el 2 % de las organizaciones perjudicadas afirmaron que menos del 1 % de sus dispositivos habían sido atacados.

Porcentaje de dispositivos afectados en la organización objeto del ataque



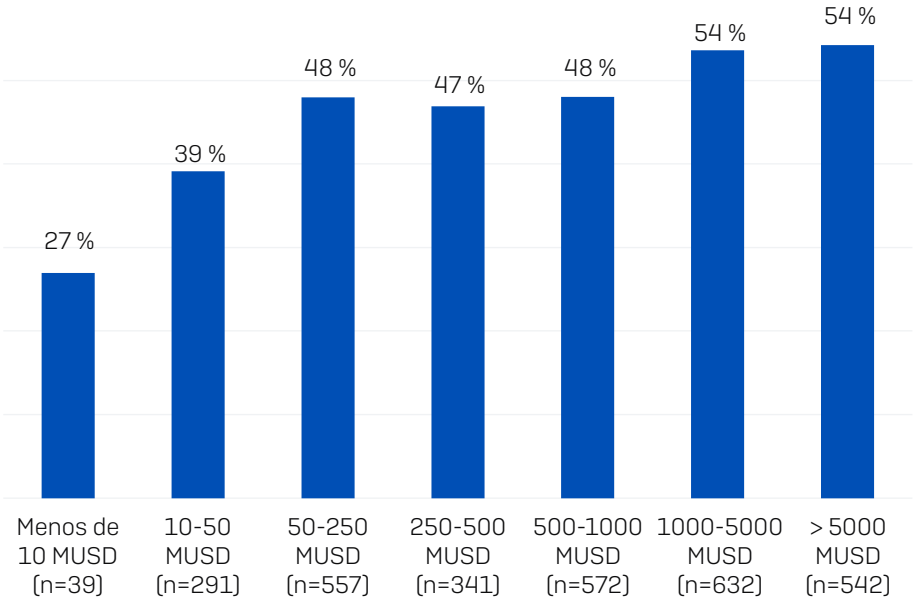
¿Qué porcentaje de los ordenadores de su organización se vieron afectados por el ransomware en el último año? n=2974 organizaciones afectadas por el ransomware.

Porcentaje de ordenadores afectados por ingresos

Aunque en términos generales la distribución entre todos los encuestados es amplia, observamos una variación significativa en los dispositivos afectados tanto por el tamaño de la organización como por el sector.

A medida que aumentan los ingresos, también lo hace la proporción del parque informático que se vio afectado en el ataque de ransomware: las organizaciones pequeñas (menos de 10 millones USD) señalaron que la mitad del porcentaje de dispositivos habían sido atacados, en comparación con aquellas con ingresos de 1000 millones USD o más (27 % frente al 54 %).

Hay varios factores que pueden contribuir a este resultado. Las organizaciones pequeñas son menos propensas a gestionar de forma centralizada todos sus dispositivos, lo que reduce la oportunidad de que los ataques se propaguen por todo el entorno. Además, la mayoría de las pequeñas empresas y empresas emergentes son grandes usuarias de plataformas SaaS, lo que reduce el riesgo de interrupción del negocio por amenazas como el ransomware.



¿Qué porcentaje de los ordenadores de su organización se vieron afectados por el ransomware en el último año? n=2974 organizaciones afectadas por el ransomware.

Porcentaje de ordenadores afectados por sector

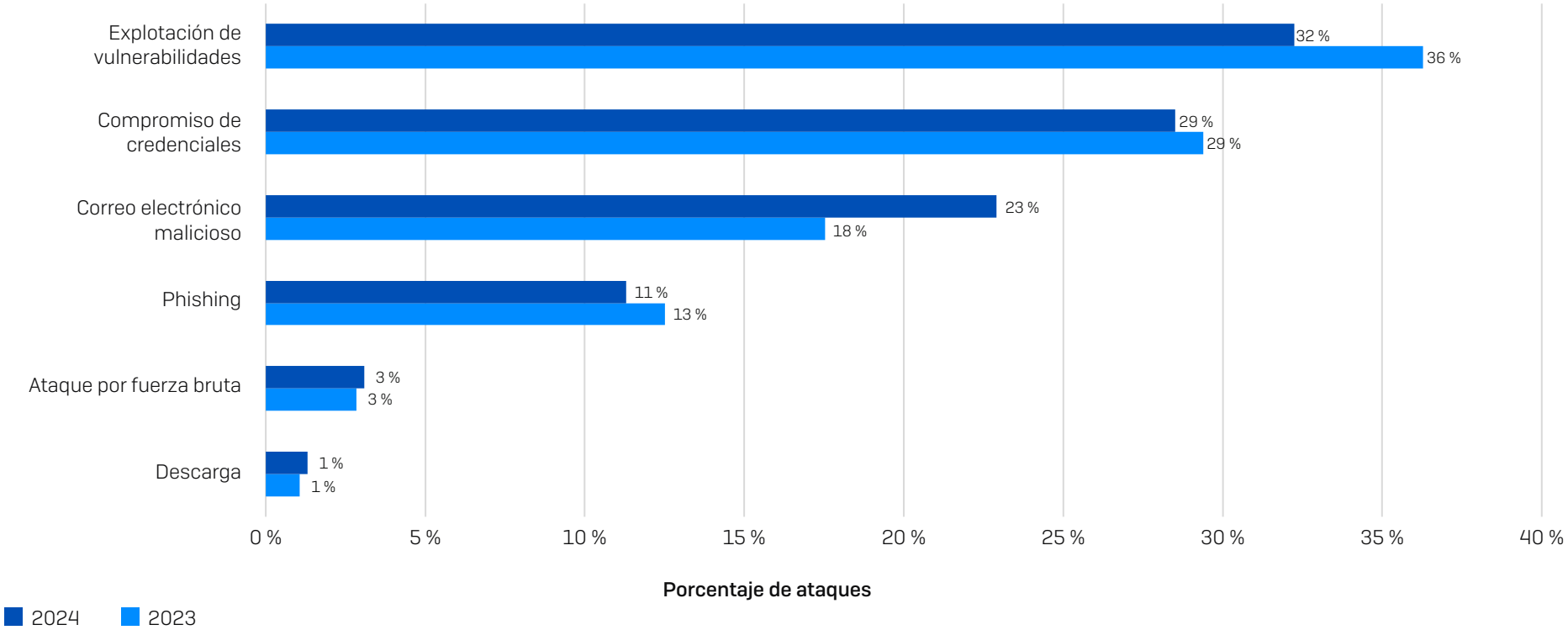
El sector de *TI, tecnología y telecomunicaciones* presentó el menor porcentaje de dispositivos afectados (33 %), lo que confirma la sólida postura de ciberseguridad que suele observarse en este sector. En el extremo opuesto, el sector de la *energía, petróleo/gas y servicios públicos* es el que sufre en mayor medida los efectos de un ataque, al verse afectados una media del 62 % de los dispositivos, seguido del *sector sanitario* (58 %). Ambos sectores tienen que lidiar con más tecnologías y controles de infraestructura heredados que la mayoría de los demás sectores, lo que probablemente hace que sea más difícil proteger los dispositivos, limitar el movimiento lateral y evitar la propagación de los ataques.

Consulte el apéndice para ver un desglose detallado del porcentaje de ordenadores afectados por sector.

Causas raíz de los ataques de ransomware

El 99 % de las organizaciones afectadas por el ransomware supieron identificar la causa raíz del ataque y, por segundo año consecutivo, la explotación de vulnerabilidades resultó ser el punto de partida más habitual. En general, el patrón siguió siendo el mismo que en nuestro estudio de 2023.

El 34 % de los encuestados señalaron las estrategias basadas en el correo electrónico como la causa raíz de los ataques, y aproximadamente el doble de estos comenzaron con un correo electrónico malicioso (un mensaje con un enlace malicioso o un archivo adjunto que descarga malware) en lugar de phishing (un mensaje que incita a los destinatarios a revelar información). Cabe señalar que el phishing se utiliza normalmente para robar datos de inicio de sesión y, como tal, puede considerarse el primer paso en un ataque de vulneración de credenciales.



¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? Sí. n=2974 organizaciones afectadas por el ransomware.

Ataques por explotación de vulnerabilidades

Aunque todos los ataques de ransomware tienen resultados negativos, algunos son más devastadores que otros. Las organizaciones cuyos ataques se iniciaron con la explotación de una vulnerabilidad sin parchear registran resultados mucho más graves, en comparación con las empresas atacadas a través de credenciales vulneradas. Estos resultados incluyen una mayor propensión a:

- Que sus copias de seguridad se vean comprometidas (índice de éxito del 75 %, frente al 54 % en el caso del compromiso de las credenciales)
- Que sus datos sean cifrados (índice de cifrado del 67 %, frente al 43 % en el caso del compromiso de las credenciales)
- Pagar el rescate (índice de pago del 71 %, frente al 45 % en el caso del compromiso de las credenciales)
- Cubrir internamente el coste total del rescate (el 31 % financió la totalidad del rescate internamente, frente al 2 % en el caso del compromiso de las credenciales)

Otros aspectos que también registraron:

- Los costes generales para recuperarse de un ataque fueron 4 veces superiores (3 millones USD, frente a los 750 000 USD en el caso del compromiso de las credenciales)
- Tardaron más en recuperarse (el 45 % tardó más de un mes, frente al 37 % en el caso del compromiso de las credenciales)

Para profundizar en el tema, consulte Vulnerabilidades sin parchear: el vector de ataque de ransomware más arrollador.

Causa raíz por sector

En algunos sectores predominan más que en otros ciertos puntos débiles en las ciberdefensas, y los adversarios no tardan en aprovecharse de ellos. En consecuencia, la causa raíz de los ataques de ransomware varía considerablemente según el sector:

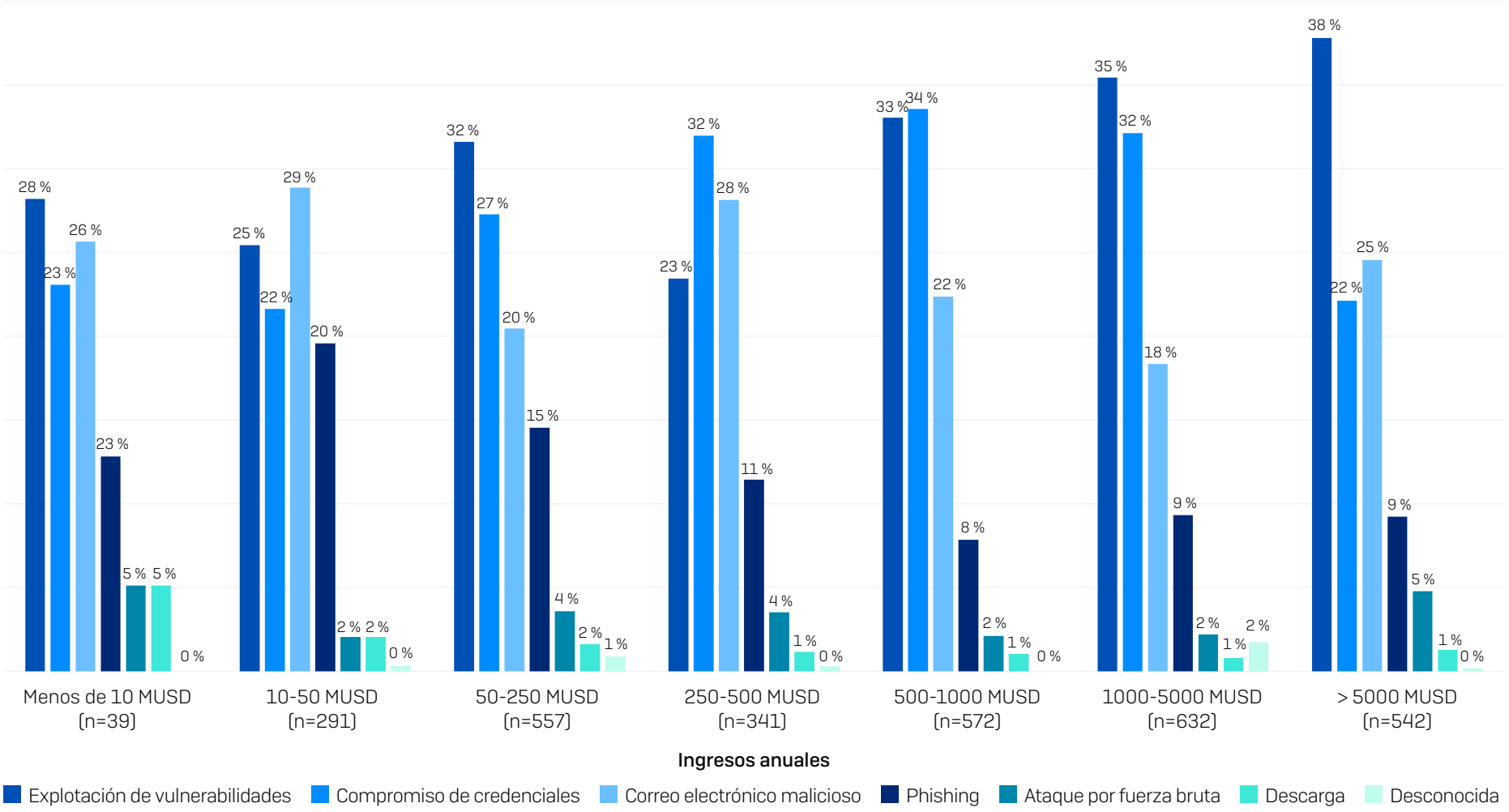
- El sector de la *energía, petróleo/gas y servicios públicos* es el que tiene más probabilidades de sufrir la explotación de vulnerabilidades sin parchear: casi la mitad (49 %) de los ataques comenzaron así. Este sector suele utilizar una mayor proporción de tecnologías antiguas y más propensas a las brechas de seguridad que muchos otros sectores, y puede que no haya parches disponibles para las soluciones heredadas y al final de su vida útil.
- Las organizaciones gubernamentales son especialmente vulnerables a los ataques que comienzan con el abuso de credenciales expuestas: El 49 % (*estatal/local*) y el 47 % (*central/federal*) de los ataques se originaron con el uso de datos de inicio de sesión robados.
- Tanto el sector de *TI, tecnología y telecomunicaciones* como el del *comercio minorista* señalaron que el 7 % de los incidentes de ransomware comenzaron con un ataque por fuerza bruta. Es posible que su menor exposición a vulnerabilidades sin parchear y credenciales comprometidas obligue a los adversarios a optar, en parte, por otros métodos.

Consulte el apéndice para ver un desglose detallado del índice de la causa raíz del ataque por sector.

Causa raíz por ingresos

En términos generales, las organizaciones de mayor tamaño tienen más probabilidades de sufrir un ataque que se inicie con una vulnerabilidad sin parchear. El tramo de ingresos de más de 5000 millones USD registra el mayor porcentaje de ataques que comenzaron de esta forma (38 %). Es probable que la infraestructura de TI aumente tanto en tamaño como en complejidad a medida que crece la organización, lo que complica a los equipos de TI el poder ver todos sus puntos vulnerables y parchearlos antes de que sean explotados.

La vulneración de credenciales como vector de ataque del ransomware se dispara en los grupos de organizaciones con ingresos medios/altos, y es la principal causa de ataque tanto en el tramo de facturación de 250-500 millones USD como en el de 500-1000 millones USD. Mientras que las vulnerabilidades y las credenciales expuestas reciben, y con razón, gran parte del protagonismo, el correo electrónico malicioso es la principal causa raíz observada en las organizaciones con ingresos de entre 10 y 50 millones USD. En líneas generales, las amenazas basadas en el correo electrónico representan algo menos de la mitad (49 %) de los ataques en esta categoría.



¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? n=2974 organizaciones afectadas por el ransomware.

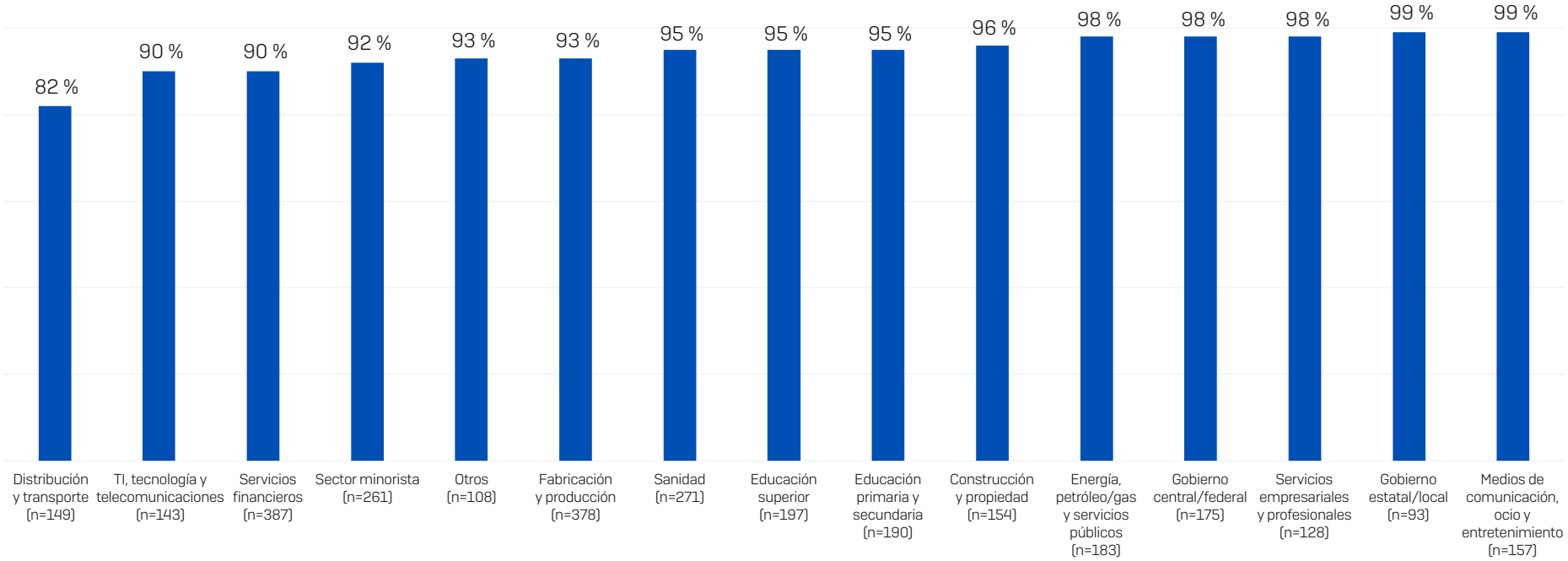
Vulneración de las copias de seguridad

Existen dos métodos principales para recuperar los datos cifrados en un ataque de ransomware: restaurarlos a partir de copias de seguridad y pagar el rescate. Al inutilizar las copias de seguridad de una organización, los adversarios restringen la capacidad de su víctima para recuperar los datos cifrados y aumentan así la presión para que pague el rescate.

Intentos de vulneración de las copias de seguridad

El 94 % de las organizaciones afectadas por el ransomware en el último año afirmaron que los ciberdelincuentes intentaron vulnerar sus copias de seguridad durante el ataque. Este porcentaje se elevó al 99 % tanto en el sector del *gobierno estatal/local* como en el de *medios de comunicación, ocio y entretenimiento*. El índice más bajo de intentos de comprometer las copias de seguridad lo registró el sector de *distribución y transporte*, aunque incluso en este caso, más de ocho de cada diez (82 %) organizaciones afectadas por el ransomware afirmaron que los atacantes intentaron acceder a sus copias de seguridad.

Porcentaje de ataques en que los adversarios intentaron vulnerar las copias de seguridad



¿Intentaron los ciberdelincuentes vulnerar las copias de seguridad de su organización? Sí. Número base en la tabla.

Índice de éxito de los intentos de vulneración de las copias de seguridad

En todos los sectores, el 57 % de los intentos de vulneración de las copias de seguridad lograron su objetivo, lo que significa que los ciberdelincuentes pudieron frustrar las actividades de recuperación del ransomware de más de la mitad de sus víctimas. Los análisis revelaron una variación significativa en el índice de éxito de los adversarios según el sector:

- El porcentaje de atacantes que consiguieron vulnerar las copias de seguridad de sus víctimas fue mayor en el sector de la *energía, petróleo/gas y servicios públicos* (índice de éxito del 79 %) y el de la *educación* (índice de éxito del 71 %).
- El sector de *TI, tecnología y telecomunicaciones* (índice de éxito del 30 %) y el de *comercio minorista* (índice de éxito del 47 %) registraron los índices más bajos de compromiso de copias de seguridad.

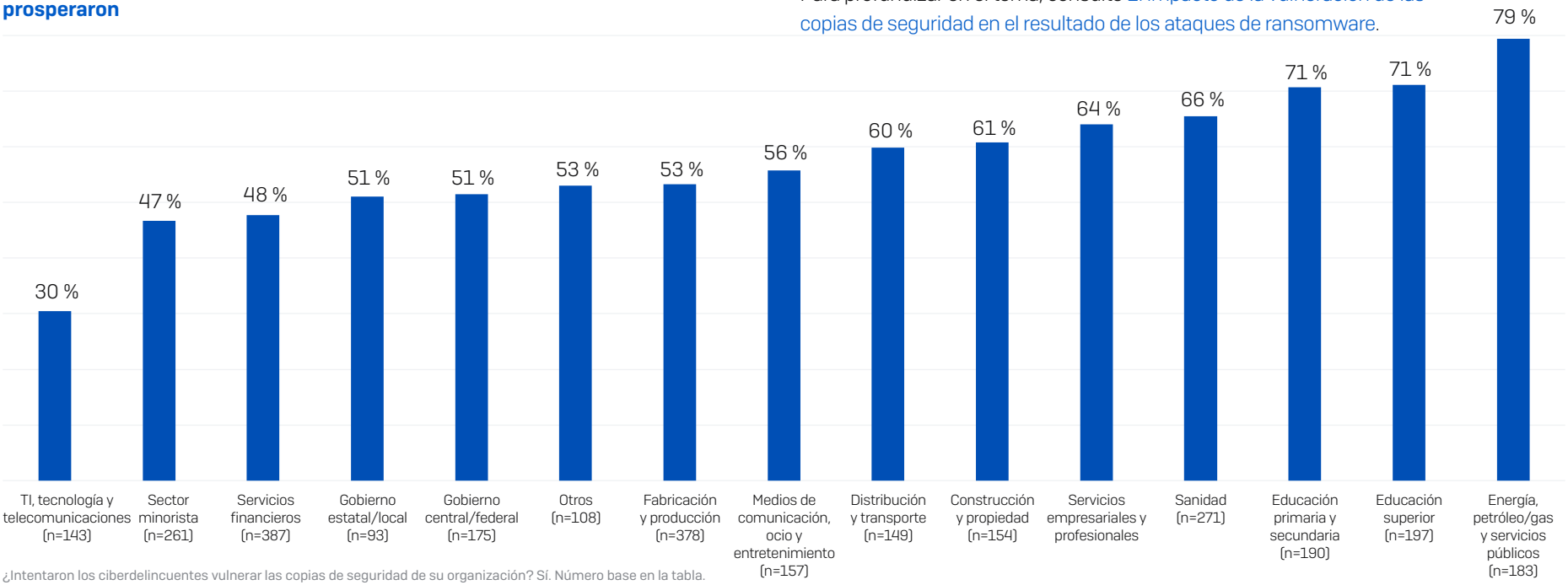
Detrás de los distintos índices de éxito hay varias razones posibles. Puede que el sector de *TI, telecomunicaciones y tecnología* contara con una protección de copias de seguridad más sólida desde un principio, por lo que era más resiliente a los ataques que otros sectores. También es posible que las organizaciones de este sector fueran más eficientes a la hora de detectar y detener los intentos de ataque antes de que los delincuentes lograran su objetivo.

Fuera cual fuera la causa, las organizaciones que vieron vulneradas sus copias de seguridad registraron resultados considerablemente peores que aquellas cuyas copias de seguridad no se vieron afectadas:

- Las peticiones de rescate fueron, de media, más del doble que las de aquellas cuyas copias de seguridad no se vieron afectadas (con una mediana de petición de rescate inicial de 2,3 millones USD frente a 1 millón USD).
- Las organizaciones cuyas copias de seguridad se vieron comprometidas tenían casi el doble de probabilidades de pagar el rescate para recuperar los datos cifrados (67 % frente al 36 %).
- La mediana de los costes globales de recuperación para las organizaciones cuyas copias de seguridad se vieron vulneradas fue ocho veces superior (3 millones USD frente a 375 000 USD).

Para profundizar en el tema, consulte El impacto de la vulneración de las copias de seguridad en el resultado de los ataques de ransomware.

Porcentaje de intentos de vulneración de las copias de seguridad que prosperaron



¿Intentaron los ciberdelincuentes vulnerar las copias de seguridad de su organización? Sí. Número base en la tabla.

Índice del cifrado de datos

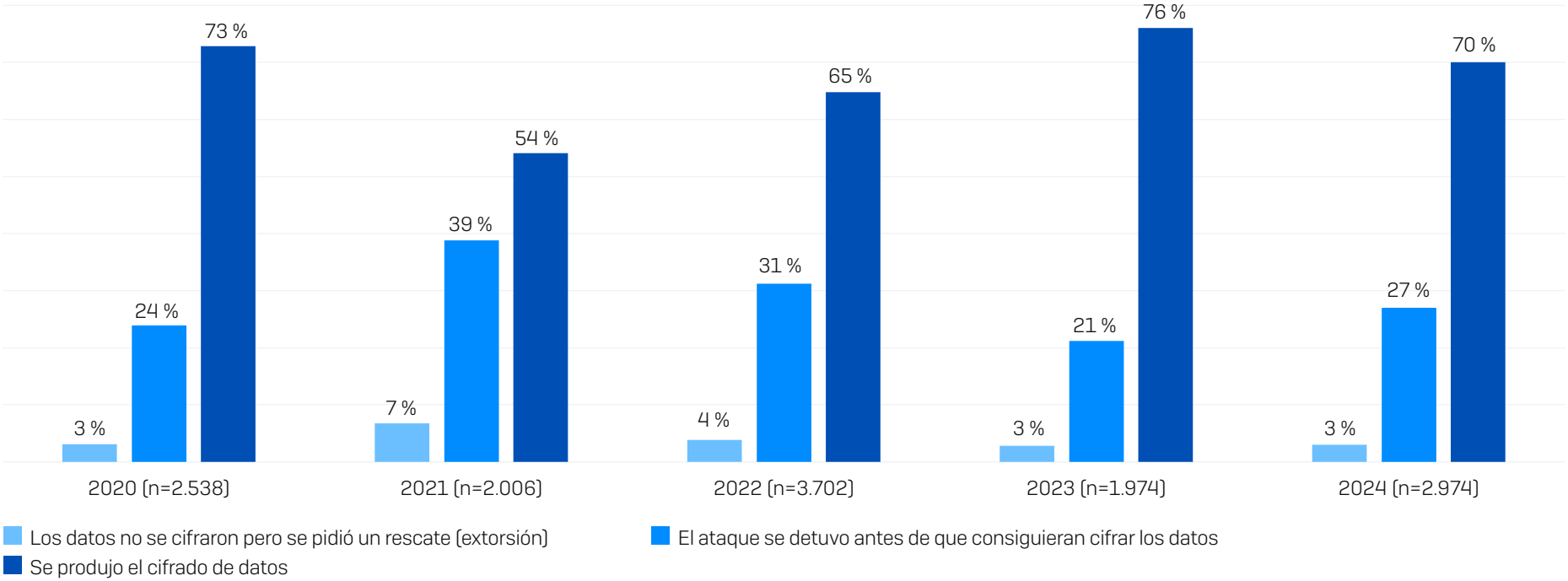
En el último año, siete de cada diez (70 %) ataques de ransomware conllevaron el cifrado de datos. Si bien este índice es elevado, representa un pequeño descenso con respecto a la cifra registrada en 2023, cuando los adversarios lograron cifrar los datos en el 76 % de los ataques.

Índice de cifrado de datos por sector

La encuesta de 2024 revela una variación considerable en el índice de cifrado de todos los sectores.

- Aunque el sector del *gobierno estatal/local* presentó la frecuencia más baja de ataques este año (el 34 % se vieron afectados por el ransomware), también registró el *índice más alto de cifrado de datos*: un 98 % de los ataques conllevaron el cifrado de datos.
- Los *servicios financieros* (49 %), seguidos del comercio minorista (56 %), registraron los *índices más bajos de cifrado de datos*.
- El sector de *distribución y transporte* es el que tiene más probabilidades de sufrir un *ataque de tipo extorsión*: un 17 % (casi el triple del índice de cualquier otro sector) afirmaron que sus datos no se cifraron, pero que se les pidió un rescate de todas formas.

Consulte el apéndice para ver un desglose detallado de los índices de cifrado de datos por sector.



¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Número base en la tabla.

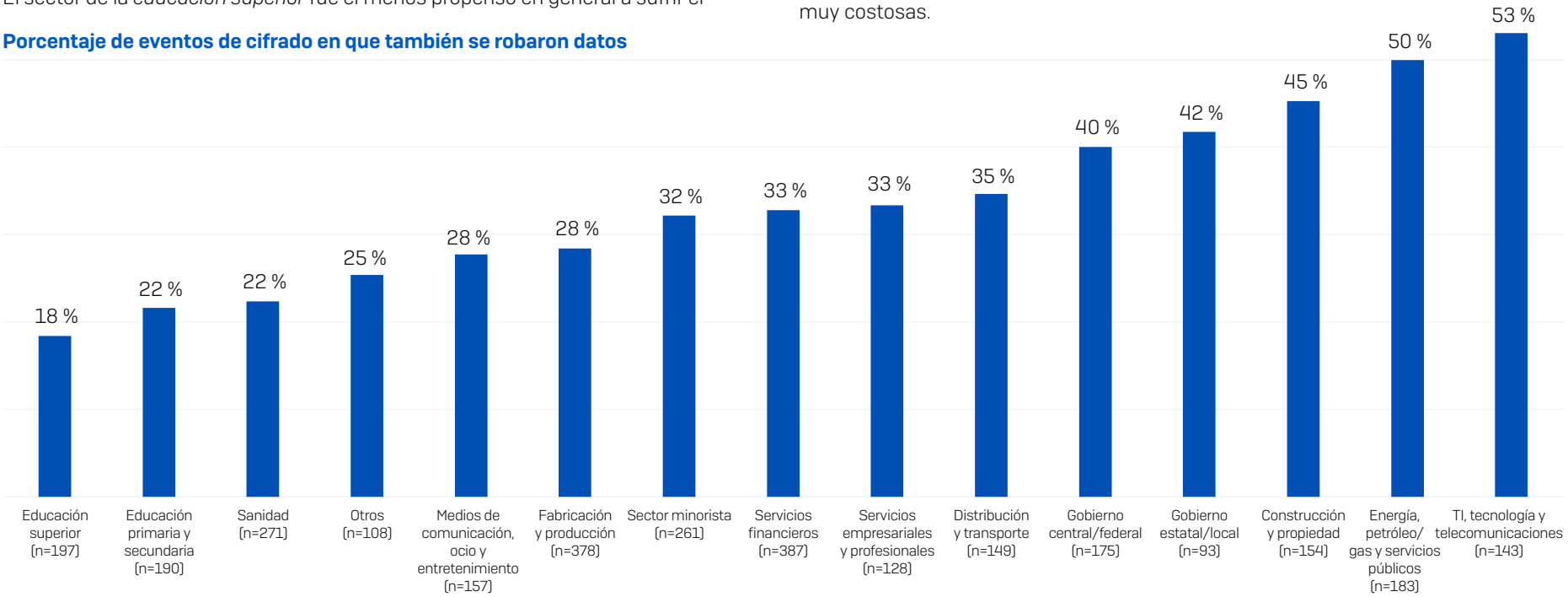
Robo de datos

Los adversarios no solo cifran los datos, sino que también los roban. En el 32 % de los incidentes en que se cifraron datos, también se produjo el robo de los datos, ligeramente por encima de la tasa del año pasado del 30%. El robo de datos aumenta la capacidad de los atacantes para extorsionar a sus víctimas, al tiempo que les permite rentabilizar aún más el ataque vendiendo los datos robados en la Web Oscura.

Una vez más, se observa una variación significativa según el sector. A primera vista, el sector de *TI, tecnología y telecomunicaciones* es el que sale peor parado, ya que en el 53 % de los ataques en que se cifraron datos, se notificó que también se robaron datos. En segundo lugar se sitúa el sector de la *energía, petróleo/gas y servicios públicos*, con un índice de robo de datos del 50 %. En el extremo opuesto, es menos probable que el sector educativo se viera afectado por el robo de datos en un ataque. El sector de la *educación superior* fue el menos propenso en general a sufrir el cifrado y el robo de datos (18 %), seguido del de la *educación primaria y secundaria*, que comparte el segundo puesto con el sector sanitario (ambos con un 22 %).

Los resultados pueden deberse a los diferentes niveles de capacidad de investigación de los distintos sectores, así como a la existencia de prioridades distintas. Determinar si se han exfiltrado datos requiere mayores niveles de capacidades forenses y a menudo depende de los registros de las herramientas EDR/XDR. Puede que el sector de *TI, tecnología y telecomunicaciones* esté simplemente mejor capacitado para identificar el robo de datos que otros sectores. La simplicidad que caracteriza muchos de los entornos del sector de la *energía, petróleo/gas y servicios públicos* también podría facilitar la detección de robos en este sector. Por otro lado, los centros educativos suelen carecer de los conocimientos y las herramientas necesarios para determinar si se han robado datos. Asimismo, es posible que algunas organizaciones prefieran no saber si se han exfiltrado datos, ya que una filtración les obligaría a hacer declaraciones muy costosas.

Porcentaje de eventos de cifrado en que 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. Número base en la tabla.

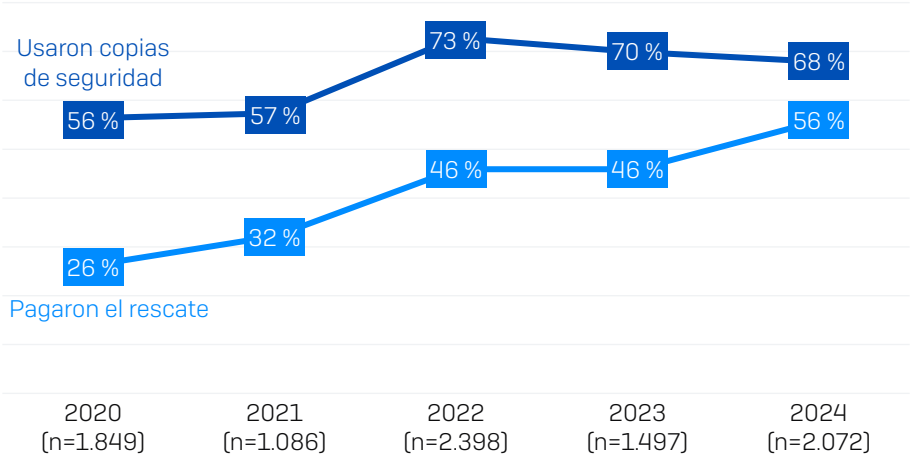
Recuperación de datos

El 98 % de las organizaciones cuyos datos fueron cifrados los recuperaron. Las dos formas principales de recuperar los datos fueron restaurarlos a partir de las copias de seguridad (68 %) y pagar el rescate para obtener la clave de descifrado (56 %). El 26 % de las organizaciones cuyos datos habían sido cifrados afirmaron haber utilizado "otros medios" para recuperarlos. Si bien la encuesta no profundizó en este aspecto, podría ser que colaboraran con las fuerzas de seguridad o que utilizaran claves de descifrado que ya se hubieran hecho públicas.

Usaron copias de seguridad para restaurar datos	Pagaron el rescate y recuperaron los datos	Usaron otros medios para recuperar datos
68 %	**56 %**	**26 %**

Un cambio destacable con respecto al año pasado es que las víctimas fueron más propensas a utilizar varios métodos para recuperar los datos cifrados (por ejemplo, pagar el rescate y usar las copias de seguridad). Casi la mitad de las organizaciones cuyos datos fueron cifrados afirmaron haber utilizado más de un método (47 %) en esta ocasión, más del doble del índice registrado en 2023 (21 %).

El gráfico que compara los últimos cinco años revela que la diferencia entre el uso de copias de seguridad y el pago del rescate sigue acortándose. Por segundo año consecutivo, el uso de copias de seguridad ha disminuido, aunque ligeramente. Al mismo tiempo, desde el estudio de 2023 se ha producido un aumento de 10 puntos porcentuales en el pago de rescates. La predisposición a pagar el rescate depende de muchos factores, entre ellos la disponibilidad de las copias de seguridad. Sin embargo, esta tendencia es preocupante y resulta inquietante que más de la mitad de las víctimas recurran a pagar por la clave de descifrado.



¿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 ingresos

La predisposición a pagar el rescate para recuperar los datos suele aumentar con los ingresos. Las organizaciones que facturan menos (menos de 10 millones USD) registran, con diferencia, el índice de pago de rescates más bajo (25 %), mientras que las organizaciones con mayores ingresos (más de 5000 millones USD) presentan el índice de pago más alto (61 %). Es muy probable que la disponibilidad fundamental de fondos para cubrir el rescate sea un factor determinante en este caso: muchas empresas pequeñas simplemente no pueden reunir el dinero para pagar un rescate.

Sin embargo, como hemos visto, en la recuperación de datos no se trata de elegir entre copias de seguridad o un rescate. Las particularidades de los métodos de recuperación de datos se hacen evidentes cuando profundizamos en los datos y comparamos las cifras de 2024 con los resultados del año pasado.

Exceptuando el grupo de organizaciones que facturan menos de 10 millones USD, todos los tramos de ingresos registraron un índice de pago de rescates superior al del año pasado, y tres de ellos también registraron un aumento en el uso de copias de seguridad para restaurar los datos. Aunque el grupo con los ingresos más bajos presentó el índice más alto de uso de copias de seguridad (88 %), las organizaciones del tramo de 250-500 millones USD le siguieron de cerca (85 %).

Recuperación de datos por sector

Quizás no sorprenda que el *gobierno central/federal* fuera el sector menos propenso a pagar el rescate para recuperar los datos (sin duda, su capacidad de pago está muy limitada por la normativa) y también el que registrara el mayor uso de copias de seguridad para restaurar los datos (39 % y 81 %, respectivamente).

En general, no existe una relación clara entre el uso de copias de seguridad y el pago de rescates:

- El sector de *medios de comunicación, ocio y entretenimiento* registró el índice más alto de pago de rescates para recuperar datos (69 %) y también uno de los índices más altos de uso de copias de seguridad (74 %).
- El sector de la *energía, petróleo/gas y servicios públicos* presentó el nivel más bajo de uso de copias de seguridad (51 %) y un índice de pago de rescates del 61 %, inferior al de otros cuatro sectores.

Consulte el apéndice para ver un desglose detallado del método de recuperación de datos por sector.

	INGRESOS ANUALES													
	Menos de 10 MUSD (n=39)		10-50 MUSD (n=291)		50-250 MUSD (n=557)		250-500 MUSD (n=341)		500-1000 MUSD (n=572)		1000-5000 MUSD (n=632)		> 5000 MUSD (n=542)	
Método de recuperación de datos utilizado	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024	2023	2024
Usaron copias de seguridad para restaurar los datos	80 %	88 % ▲	72 %	68 % ▼	77 %	60 % ▼	75 %	85 % ▲	68 %	70 % ▲	66 %	65 % ▼	63 %	66 % ▲
Pagaron el rescate y recuperaron los datos	36 %	25 % ▼	41 %	49 % ▲	42 %	57 % ▲	33 %	50 % ▲	51 %	59 % ▲	52 %	56 % ▲	55 %	61 % ▲

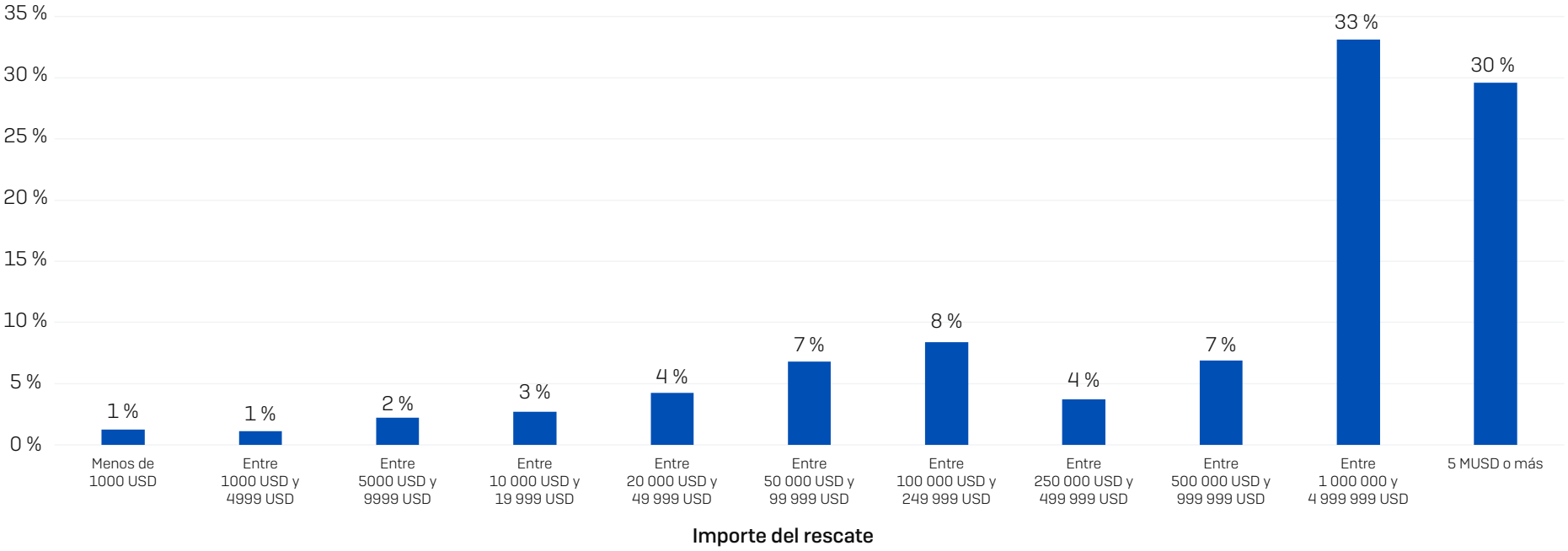
¿Recuperó su organización los datos? Sí, pagamos el rescate y recuperamos los datos; Sí, usamos copias de seguridad para restaurar los datos. Números base de 2024 en la tabla. La flecha indica el aumento o la disminución respecto a 2023.

Peticiones de rescate

Este año, por primera vez, hemos incluido en el informe tanto las peticiones de rescate como los pagos. 1701 organizaciones cuyos datos fueron cifrados compartieron la petición inicial de rescate de los delincuentes: la media ascendió a 4 321 880 USD y, la mediana, a 2 millones USD.

Un dato del estudio de este año que es digno de mención es que el 63 % de las peticiones de rescate ascendieron a 1 millón USD o más, y el 30 % de ellas se dispararon a 5 millones USD o más. Aunque un pequeño número de encuestados comunicaron peticiones de rescate de cuatro cifras, son una minoría.

Porcentaje de peticiones de rescate por importe



¿A cuánto ascendía el rescate exigido por los atacantes? n=1701

Petición de rescate por ingresos

Si se observan tanto la media como la mediana, la petición de rescate muestra una tendencia al alza con los ingresos, lo que indica que los adversarios ajustan su petición de rescate basándose, al menos en parte, en la posible capacidad de pago.

Las peticiones de rescate de gran cuantía ya no son exclusivas de las organizaciones con los ingresos más elevados, y las peticiones de 1 millón USD o más son ahora habituales de forma generalizada: el año pasado, el 47 % de las organizaciones con ingresos de entre 10 y 50 millones USD recibieron una petición de rescate de siete cifras.

Petición de rescate por sector

Aquí no hay ganadores, ya que todos los sectores mencionados (excepto el de "otros") registraron una mediana de peticiones de rescate de 1 millón USD o más.

- El sector del *comercio minorista* y el de *TI, tecnología y telecomunicaciones* recibieron las peticiones más bajas, con una mediana de 1 millón USD, seguidos del de la *construcción* (1,1 millones USD).
- El sector del *gobierno central/federal* es el que atrajo las peticiones de rescate más altas: una mediana de 7,7 millones USD y una media de 9,9 millones USD.

Consulte el apéndice para ver un desglose detallado de las peticiones de rescate por sector.

	INGRESOS ANUALES					
Petición de rescate	**10-50 MUSD (n=207)**	**50-250 MUSD (n=288)**	**250-500 MUSD (n=158)**	**500-1000 MUSD (n=268)**	**1000-5000 MUSD (n=366)**	**> 5000 MUSD (n=398)**
Media	1 774 941 USD	1 704 853 USD	3 407 796 USD	5 184 024 USD	4 281 258 USD	7 467 294 USD
Mediana	330 000 USD	220 000 USD	840 000 USD	2 000 000 USD	3 000 000 USD	6 600 000 USD

¿A cuánto ascendía el rescate exigido por los atacantes? Números base en la tabla. Nota: se ha excluido de la tabla "Menos de 10 MUSD" debido a una base de respuestas baja en este tramo de ingresos.

Importes de rescate

Un total de 1097 encuestados cuya organización pagó el rescate compartieron el importe que realmente pagaron. Si observamos la mediana y la media, vemos que el importe de rescate pagado ha aumentado considerablemente en el último año:

- Mediana del importe pagado: 2 000 000 USD (la cifra de 400 000 USD de 2023 se multiplica por 5)
- Media del importe pagado: 3 960 917 USD (la cifra de 1 542 330 USD de 2023 se multiplica por 2,6)

El gráfico siguiente evidencia cómo la proporción de importes de rescate muy bajos ha disminuido progresivamente en los últimos tres años, mientras que la proporción de importes muy elevados se ha disparado. Ahora, pagar un rescate de siete cifras o más es la norma.

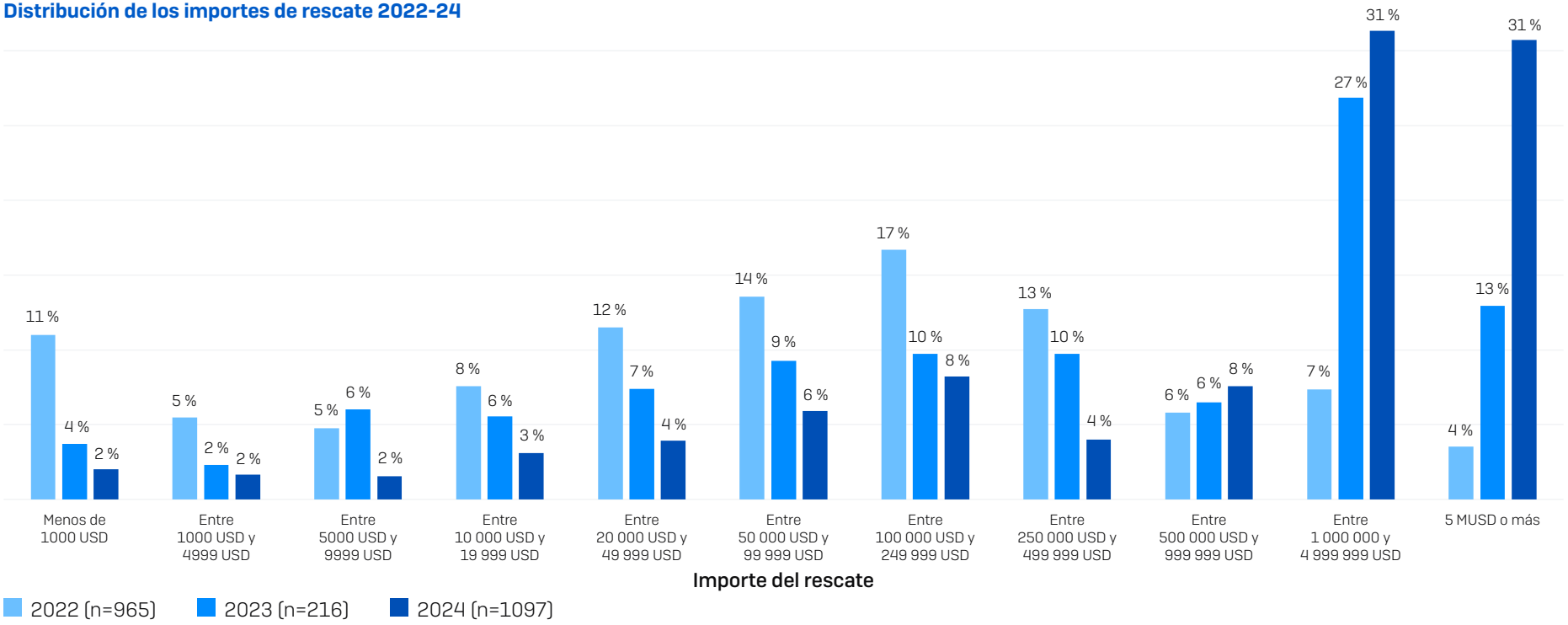
Importes de rescate por sector

Al igual que el promedio de peticiones de rescate varía considerablemente según el sector, también lo hace el importe. El sector de *TI, tecnología y telecomunicaciones* registró la mediana del importe de rescate más baja (300 000 USD), seguido por el de *distribución y transporte* (440 000 USD). En el extremo opuesto, tanto el sector de la *educación primaria y secundaria* como el del *gobierno central/federal* pagaron una mediana de rescate de 6,6 millones USD.

Aunque existe una correlación general entre las peticiones más bajas y los pagos más bajos (y viceversa), hay excepciones, sobre todo en el sector de *distribución y transporte*, cuya mediana de petición de rescate se situó por encima de los 2,8 millones USD, pero pagó, de media, 440 000 USD.

Consulte el apéndice para ver un desglose detallado del importe de rescate medio por sector.

Distribución de los importes de rescate 2022-24



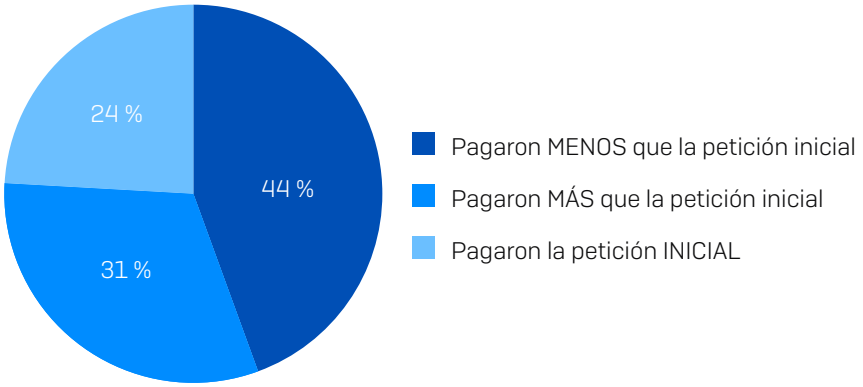
¿Cuál fue el importe del rescate que pagó su organización a los atacantes? Números base en la tabla.

Petición de rescate frente al importe de rescate

Cuando los datos se cifran, es un momento de enorme presión para todas las partes implicadas, ya que ambas intentan optimizar sus resultados. Las organizaciones con datos cifrados tratan de minimizar el impacto financiero, mientras que los adversarios intentan sacar el máximo dinero posible en el menor tiempo posible, a menudo presionando aún más con la amenaza de que el rescate aumentará si no se paga en un plazo determinado.

Propensión a negociar el importe de rescate

El estudio ha revelado que las víctimas pocas veces pagan la suma inicial exigida por los atacantes: solo el 24 % de los encuestados afirma que el importe que pagaron coincidió con la petición original. El 44 % pagó menos que la petición inicial, mientras que el 31 % pagó más.



¿A cuánto ascendía el rescate exigido por los atacantes? ¿Cuál fue el importe de rescate que pagó su organización a los atacantes? n=1097.

Si observamos los datos por sectores, vemos que los dos sectores de servicios (*servicios empresariales y profesionales* y *servicios financieros*) fueron los más propensos a negociar a la baja el importe de rescate, y un 67 % afirmó haber pagado menos que la petición inicial. El sector de *fabricación y producción* va a la zaga, con un índice del 65 %.

Por el contrario, los sectores más propensos a pagar más que la petición inicial son los que tienen una elevada proporción de organizaciones del sector público:

- El de la *educación superior* fue el más propenso a pagar una cantidad superior a la exigida originalmente (el 67 % pagó más) y el menos propenso a pagar una cantidad inferior a la exigida inicialmente (el 20 % pagó menos).
- El *sector sanitario* fue el segundo más propenso a pagar por encima de la petición inicial (el 57 % pagó más), seguido del de la *educación primaria y secundaria* (el 55 % pagó más).

Puede que estos sectores tengan menos acceso a negociadores profesionales de rescates que les ayuden a reducir sus costes. También es posible que tengan una mayor necesidad de recuperar los datos "a toda costa" debido a su cometido público. En cualquier caso, es evidente que hay margen de maniobra entre la petición original y el pago final.

Consulte el apéndice para ver un desglose detallado de la petición de rescate frente al importe de rescate por sector.

Proporción pagada del rescate exigido

Aunque en la mayoría de los casos se negocia el importe de rescate, el margen de maniobra final es relativamente pequeño: de todo el conjunto, los encuestados afirmaron haber pagado, de media, el 94 % de la petición inicial.

Si ahondamos un poco más, vemos que todos los tramos de ingresos, excepto el más alto, lograron reducir la cuantía del rescate. El tramo de 50 a 250 millones USD pagó la proporción más baja de la petición inicial (84 %). El único grupo que pagó más que la petición inicial es el tramo de ingresos de más de 5000 millones USD, que abonó, de media, el 115 % del importe exigido.

	INGRESOS ANUALES					
Tramo	**10-50 MUSD (n=100)**	**50-250 MUSD (n=206)**	**250-500 MUSD (n=104)**	**500-1000 MUSD (n=175)**	**1000-5000 MUSD (n=233)**	**> 5000 MUSD (n=275)**
Proporción pagada del rescate exigido	93 %	84 %	90 %	88 %	85 %	115 %

¿A cuánto ascendía el rescate exigido por los atacantes? ¿Cuál fue el importe de rescate que pagó su organización a los atacantes? n=1097. Nota: el tramo de ingresos de "menos de 10 MUSD" se excluye del desglose de ingresos anuales porque tiene una base de respuestas muy baja.

Proporción pagada del rescate exigido por sector

A nivel sectorial, observamos que los sectores más propensos a negociar a la baja el importe del rescate también pagan el porcentaje más bajo de la petición inicial, y viceversa.

MENOS DEL 100 %	MÁS DEL 100 %
Fabricación y producción (70 %)	Educación superior (122 %)
Servicios empresariales y profesionales (74 %)	Educación primaria y secundaria (115 %)
Servicios financieros (75 %)	Sanidad (111 %)
Otros (79 %)	Gobierno estatal/local (104 %)
TI, tecnología y telecomunicaciones (82 %)	Gobierno central/federal (103 %)
Comercio minorista (84 %)	Energía, petróleo/gas y servicios públicos (101 %)
Construcción y propiedad (95 %)	
Distribución y transporte (95 %)	
Medios de comunicación, ocio y entretenimiento (95 %)	

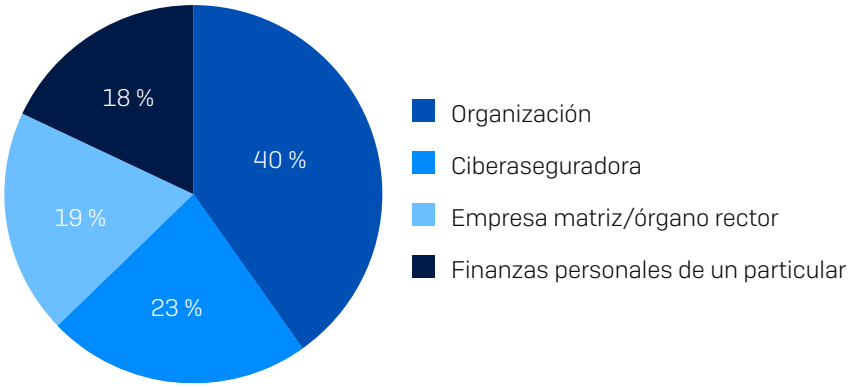
¿A cuánto ascendía el rescate exigido por los atacantes? ¿Cuál fue el importe de rescate que pagó su organización a los atacantes? n=1097.

Fuente de financiación de los rescates

Quién financia el rescate es un tema de gran interés, y el estudio ha revelado varias conclusiones al respecto:

- La financiación del rescate es un esfuerzo colectivo: los encuestados mencionaron múltiples fuentes de dinero en más de cuatro quintas partes (82 %) de los casos.
- La principal fuente de financiación de los rescates es la propia organización, que cubre, de media, el 40 % del importe; la empresa matriz y/o el órgano rector de la organización suelen aportar el 19 %.
- Las aseguradoras intervienen de forma notable en el pago de los rescates:
  - El 23 % de la financiación del pago de rescates procede de compañías de seguros.
  - Las aseguradoras ayudan a pagar el rescate en el 83 % de los ataques.
  - Sin embargo, las aseguradoras muy pocas veces (1 %) cubren el importe total y, en el 79 % de los casos, financiaron menos de la mitad del desembolso total.

Fuente de financiación del pago del rescate



¿De cuál o cuáles de las siguientes fuentes se obtuvo el dinero para financiar el pago del rescate? n=1168.

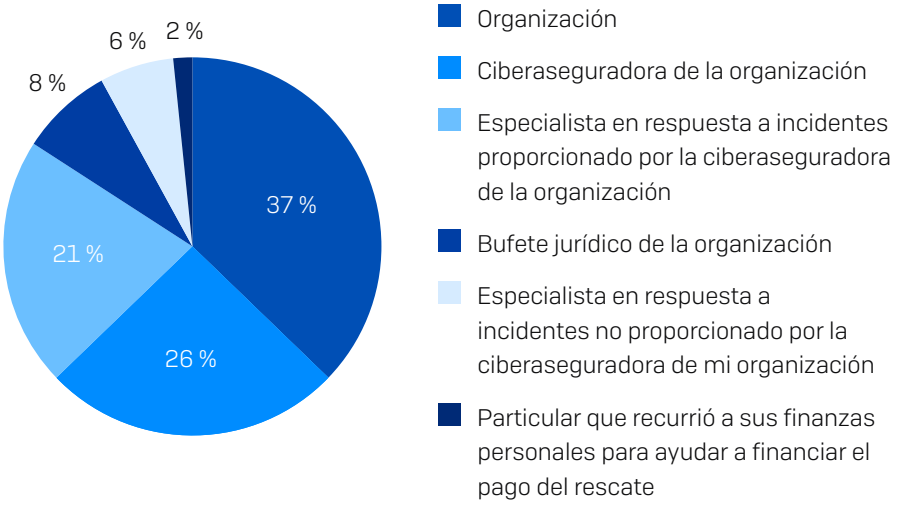
Ejecución de la transacción del pago del rescate

Aunque varias entidades pueden ayudar a pagar el rescate, los fondos los suele transferir una sola parte en un único pago.

En términos globales, las aseguradoras transfirieron los fondos de casi la mitad de los pagos de rescates, bien directamente (26 %) o a través de su especialista en respuesta a incidentes designado (21 %). La organización afectada efectuó el 37 % de los pagos, mientras que el 8 % fue ejecutado por el bufete jurídico de la víctima.

En general, el 28 % (redondeando) de las transferencias fueron realizadas por especialistas en respuesta a incidentes, ya fueran designados por la aseguradora (21 %) o por otra parte, normalmente la víctima (6 %).

Ejecutante de la transferencia del pago del rescate



¿Quién se encargó de la transacción del pago del rescate, es decir, quién transfirió el dinero a la cuenta del atacante? n=1168.

Costes de recuperación

El pago de rescates es solo un elemento de los costes de recuperación en la gestión de los eventos de ransomware. Sin contar los rescates pagados, en 2024 el coste medio de recuperación de las organizaciones tras un ataque de ransomware fue de 2,73 millones USD, lo que supone un aumento de casi 1 millón USD con respecto a los 1,82 millones USD de 2023.

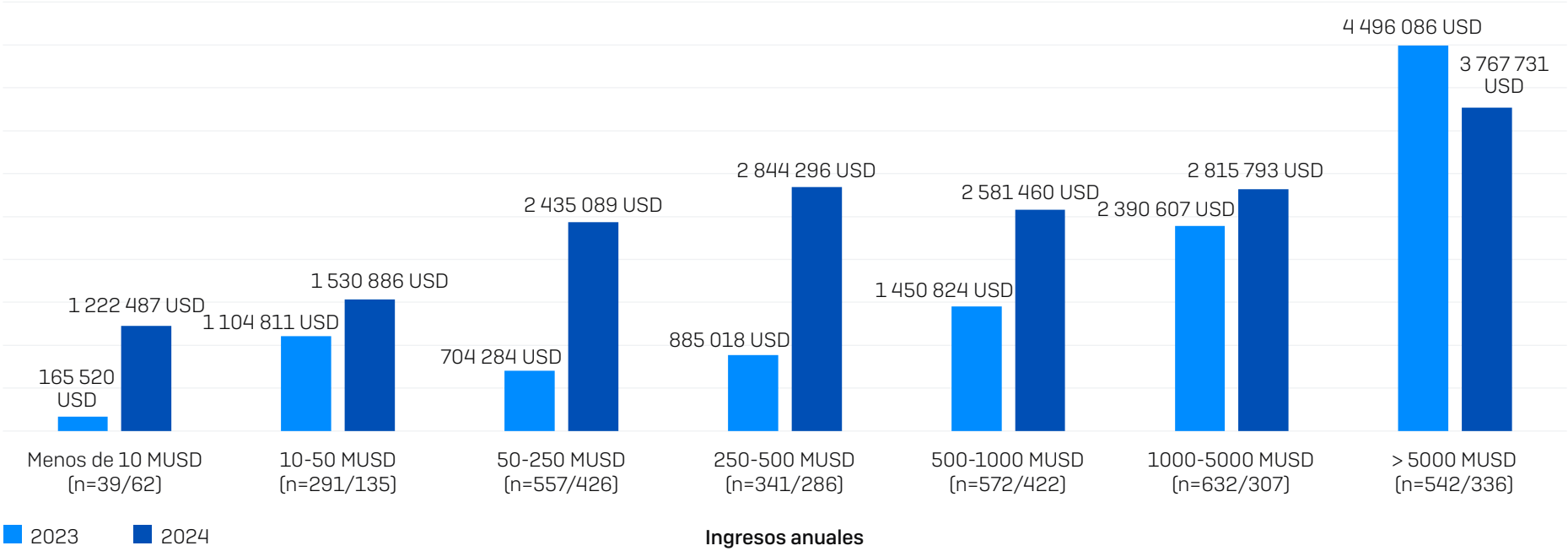
2021	2022	2023	2024
1,85 MUSD	1,4 MUSD	1,82 MUSD	2,73 MUSD

¿Cuál fue el coste aproximado que tuvo que asumir su 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=2974 (2024) /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 tramos de organizaciones de ingresos bajos y medios experimentaron el mayor incremento de los costes generales de recuperación, y el tramo de ingresos entre 250 y 500 millones USD registró el mayor aumento individual, de 2 millones USD (de 885 018 a 2 885 296 USD).

Las organizaciones con una facturación de entre 1000 y 5000 millones USD registraron un aumento (relativamente) pequeño de poco más de 400 000 USD, mientras que las organizaciones más grandes, con una facturación anual superior a 5000 millones USD, fueron las únicas que vieron reducido su coste de recuperación, pasando de 4 496 096 USD a 3 767 731 USD.

El análisis de la mediana del coste de recuperación confirma las tendencias. A nivel mundial, en el último año se duplicó la mediana de los costes de recuperación, pasando de 375 000 a 750 000 USD. El aumento de los costes se produjo sobre todo en los cinco tramos de ingresos más bajos, que registraron una subida considerable, mientras que en los dos tramos de ingresos más elevados los costes se mantuvieron relativamente estables.



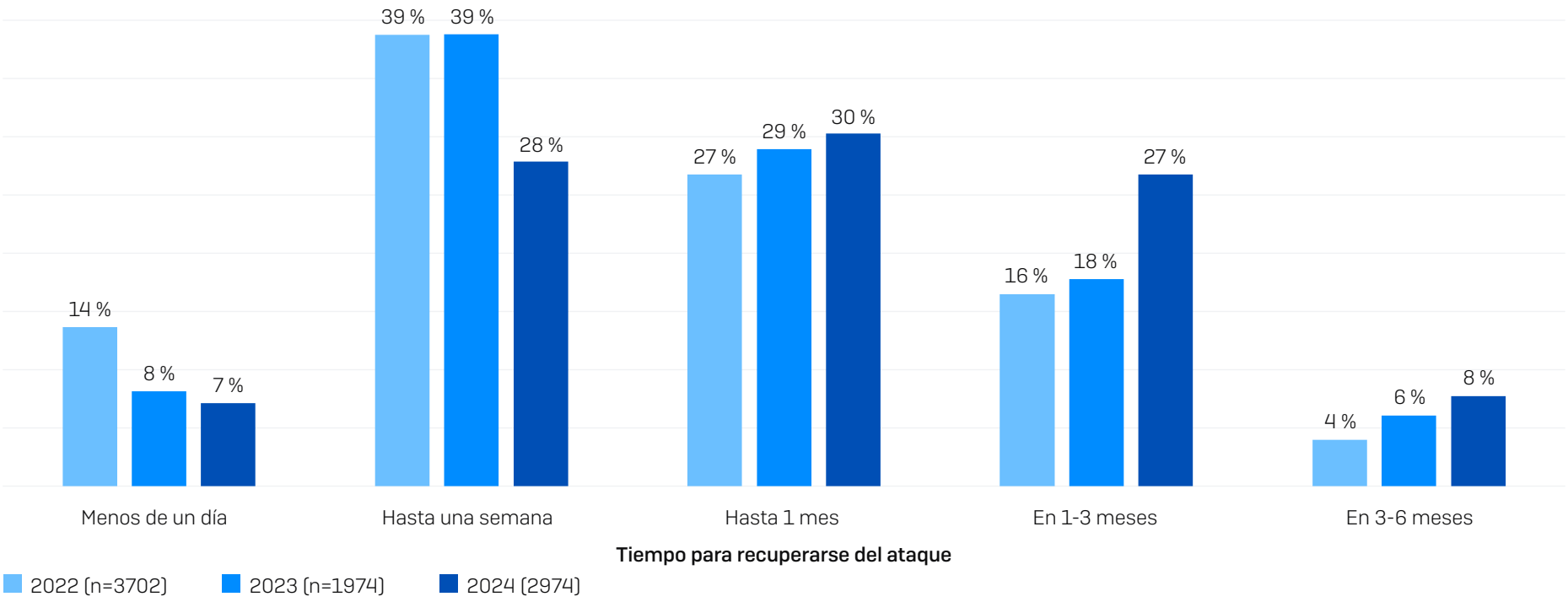
¿Cuál fue el coste aproximado que tuvo que asumir su organización para rectificar los perjuicios del ataque de ransomware más significativo (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, etc.)? n=2974 (2024), 1974 (2023). Números base de 2023/2024, por ingresos, en el gráfico.

Tiempo de recuperación

El tiempo necesario para recuperarse de un ataque de ransomware es cada vez más largo. Nuestra investigación de 2024 ha revelado lo siguiente:

- El 35 % de las víctimas del ransomware se recuperan totalmente en una semana o menos, lo que supone un descenso respecto al 47 % de 2023 y al 52 % de 2022.
- Un tercio (34 %) tarda ahora más de un mes en recuperarse, lo que representa un aumento con respecto al 24 % de 2023 y al 20 % de 2022.

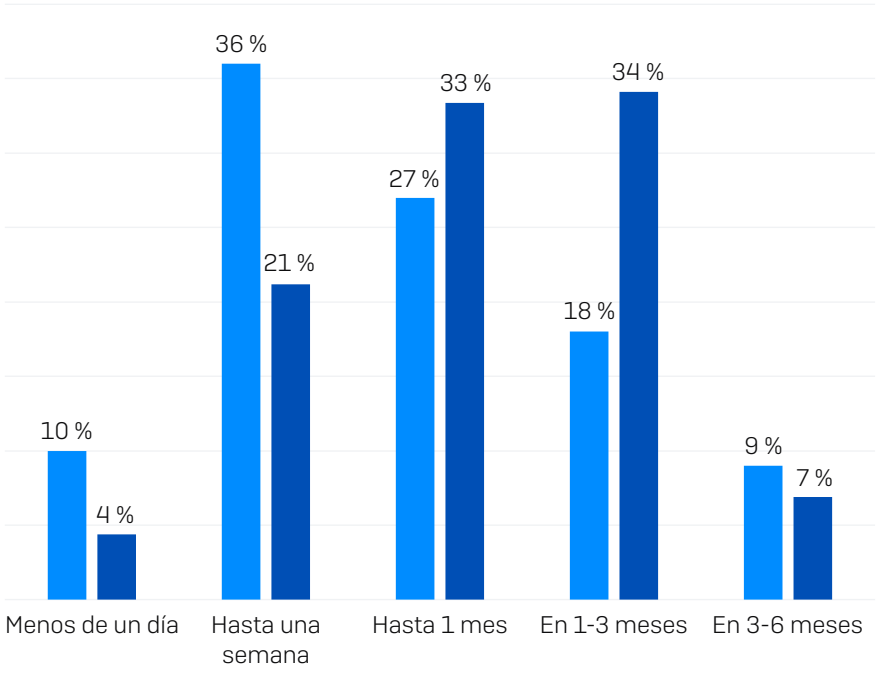
Esta ralentización puede obedecer a la mayor complejidad y gravedad de los ataques, que hacen necesario un mayor trabajo de recuperación. También puede indicar que las organizaciones se preparan cada vez menos para recuperarse de un ataque.



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

Tiempo de recuperación: impacto de la vulneración de las copias de seguridad

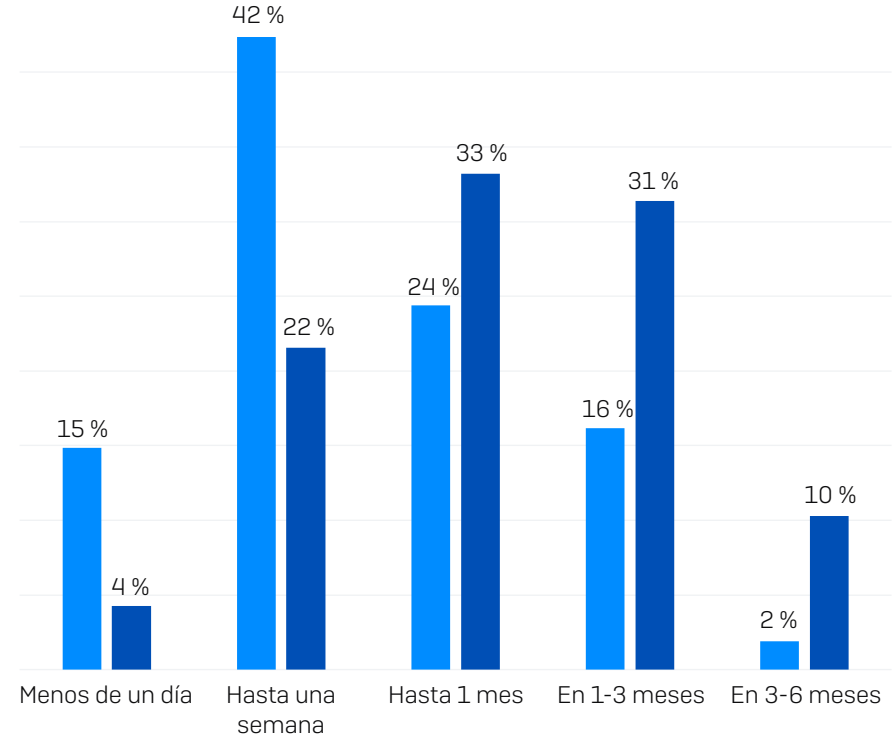
El hecho de que sus copias de seguridad se vean vulneradas repercute enormemente en el tiempo total de recuperación. Casi la mitad de las organizaciones cuyas copias de seguridad permanecieron intactas se recuperaron en una semana o menos (46 %), en comparación con una cuarta parte (25 %) de aquellas cuyas copias de seguridad se vieron afectadas. Si sus copias de seguridad se ven comprometidas, aumenta la complejidad de la recuperación de los datos cifrados, además de sumarse los gastos de crear y proteger nuevas copias de seguridad intactas.



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

Tiempo de recuperación: impacto del cifrado de datos

No es de extrañar que sufrir el cifrado de los datos en un ataque aumente significativamente el tiempo de recuperación. El 57 % de las organizaciones cuyos datos no fueron cifrados se recuperaron por completo en el plazo de una semana, frente al 25 % de aquellas cuyos datos sí fueron cifrados.

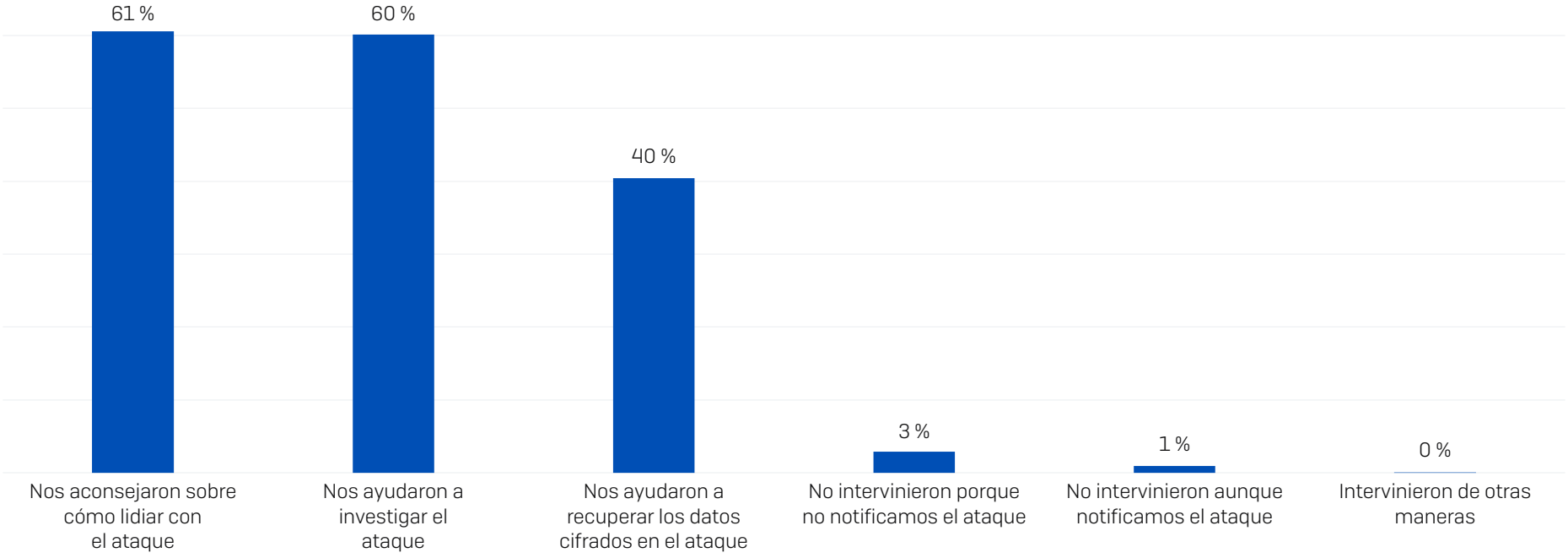


¿Cuánto tiempo tardó su organización en recuperarse totalmente del ataque de ransomware? Números base en la tabla.

Implicación de las autoridades y fuerzas del orden

El tipo y la disponibilidad de apoyo oficial a la hora de hacer frente a un ataque de ransomware varían de un país a otro, al igual que las herramientas para notificar un ciberataque. Las víctimas estadounidenses pueden recurrir a la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA); las del Reino Unido, al Centro Nacional de Ciberseguridad (NCSC); y las organizaciones australianas, al Centro Australiano de Ciberseguridad (ACSC), por citar solo algunos ejemplos.

El 97 % de las organizaciones de todo el mundo que se vieron afectadas por el ransomware se pusieron en contacto con las fuerzas del orden y/o los organismos gubernamentales oficiales debido al ataque, lo que evidencia la normalización del ransomware. El 61 % afirmaron haber recibido asesoramiento para lidiar con el ataque, el 60 % obtuvieron ayuda para investigar el ataque y el 40 % recibieron asistencia para recuperarse del ataque.

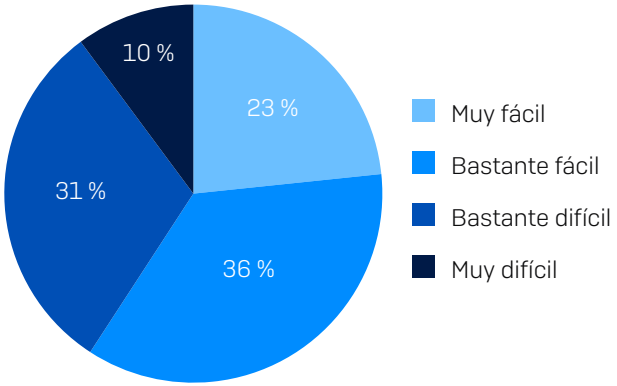


Cómo intervinieron las fuerzas del orden y/o los organismos gubernamentales

Si su organización notificó el ataque a las fuerzas del orden y/o a un organismo gubernamental oficial, ¿qué tipo de intervención llevaron a cabo? n=2974.

Facilidad para entablar contacto

Resulta alentador que más de la mitad (59 %) de las organizaciones que contactaron con las fuerzas del orden y/o los organismos oficiales a raíz del ataque dijeran que el proceso había sido fácil (23 % muy fácil, 36 % bastante fácil). Solo el 10 % manifestaron que el proceso había sido muy difícil, y el 31 % lo describieron como bastante difícil.



¿Le resultó fácil o difícil a su organización contactar con las fuerzas del orden y/o los organismos oficiales en relación con el ataque? n=2874 (Se excluyen las respuestas "No lo sé").

No implicación de los organismos oficiales

Hubo una serie de razones por las que el 3 % (86 encuestados) no comunicaron el ataque, y las dos más frecuentes fueron la preocupación de que tuviera un impacto negativo en su organización, como multas, gastos o trabajo extra (27 %), y porque pensaban que no les reportaría ningún beneficio (también 27 %). Varios encuestados afirmaron textualmente que no recurrieron a los organismos oficiales porque pudieron resolver el problema a nivel interno.

Nos preocupaba que tuviera un impacto negativo en nuestra organización, por ejemplo, multas, gastos o trabajo extra	**27 %**
Pensamos que informar del ataque no reportaría ningún beneficio a nuestra organización	**27 %**
Pensamos que no les interesaría el ataque	**22 %**
Estábamos demasiado ocupados lidiando con el ataque como para pensar en involucrarlos	**21 %**
Los atacantes nos advirtieron que no nos dirigiéramos a ellos	**19 %**
No sabíamos a qué fuerzas del orden u organismos oficiales involucrar	**10 %**
No teníamos la obligación legal de informar del ataque	**9 %**
Otras (especifique)	**3 %**
No lo saben	**1 %**

¿Por qué no denunció su organización el ataque a las fuerzas del orden y/o a los organismos oficiales? (n=86).

Conclusión

El ransomware sigue siendo una grave amenaza para organizaciones de todos los tamaños de todo el mundo. Si bien el índice general de ataques ha disminuido en los dos últimos años, ha aumentado el impacto que tiene un ataque sobre quienes lo sufren. A medida que los adversarios continúan redoblando y perfeccionando sus ataques, es esencial que los encargados de la seguridad y sus ciberdefensas sigan el ritmo.

Prevención. El mejor ataque de ransomware es aquel que no se llega a producir porque los adversarios no consiguen entrar en su organización. Dado que un tercio de los ataques comienzan con la explotación de vulnerabilidades sin parchear, es importante tomar el control de la superficie de ataque e implementar una priorización de los parches basada en el riesgo. El uso de MFA para limitar el abuso de credenciales también debe ser una prioridad para todas y cada una de las organizaciones. Asimismo, sigue siendo fundamental la formación continua de los usuarios sobre cómo detectar el phishing y los correos electrónicos maliciosos.

Protección. Es imprescindible contar con una base sólida de seguridad, que incluya tecnologías para endpoints, correo electrónico y firewalls. Los endpoints (incluidos los servidores) son el objetivo principal de los operadores de ransomware, así que procure que estén debidamente blindados, incluida una protección específica antiransomware para detener y revertir el cifrado malicioso. Las herramientas de seguridad deben configurarse y desplegarse correctamente para ofrecer una protección óptima. Busque soluciones listas para usar con controles sencillos para gestionar la postura de seguridad. Una protección compleja y difícil de desplegar puede aumentar fácilmente el riesgo en lugar de reducirlo.

Detección y respuesta. Cuanto antes detenga un ataque, mejor. Detectar y neutralizar a un adversario dentro de su entorno antes de que pueda vulnerar sus copias de seguridad o cifrar sus datos mejorará considerablemente sus resultados.

Planificación y preparación. Contar con un plan de respuesta a incidentes que sepa bien cómo implementar mejorará en gran medida sus resultados si llega a ocurrir lo peor y sufre un ataque importante. Practique con regularidad la restauración de datos a partir de las copias de seguridad para garantizar agilidad y soltura en caso de que tenga que actuar tras un ataque.

Para descubrir cómo Sophos puede ayudarle a optimizar sus defensas contra el ransomware, hable con un asesor o visite es.sophos.com

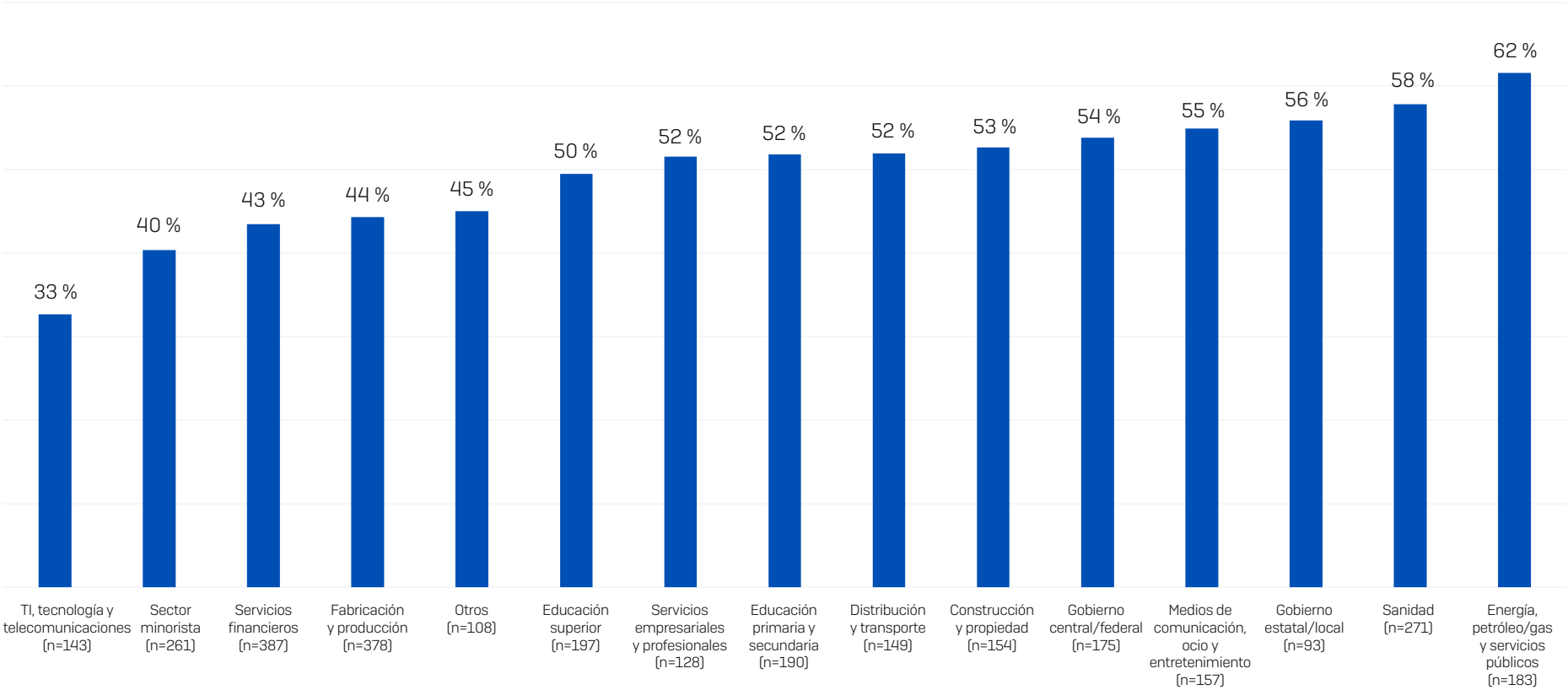
Acerca de Vanson Bourne

Vanson Bourne es una consultora independiente especializada en estudios de mercado para el sector tecnológico. Su reputación de análisis sólidos y creíbles basados en la investigación se asienta en rigurosos principios de investigación y en su capacidad para recabar las opiniones de los principales responsables de la toma de decisiones en todas las funciones técnicas y empresariales, en todos los sectores empresariales y en todos los principales mercados. Si desea más información, visite www.vansonbourne.com.

Apéndice

Porcentaje de ordenadores afectados por sector

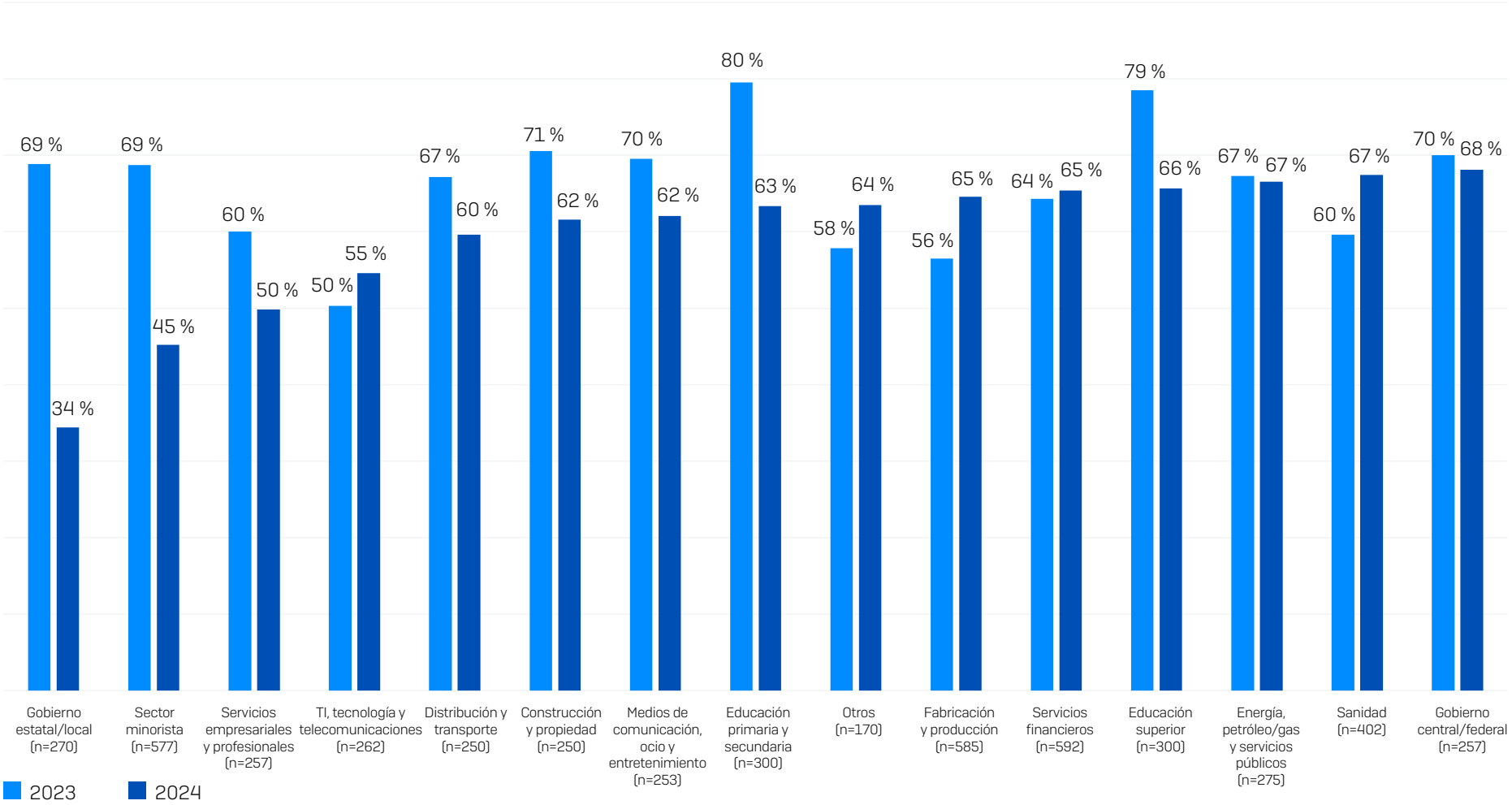
Porcentaje de dispositivos afectados



¿Qué porcentaje de los ordenadores de su organización se vieron afectados por el ransomware en el último año? n=2974 organizaciones afectadas por el ransomware. Números base por sector en el gráfico.

Índice de los ataques de ransomware por sector

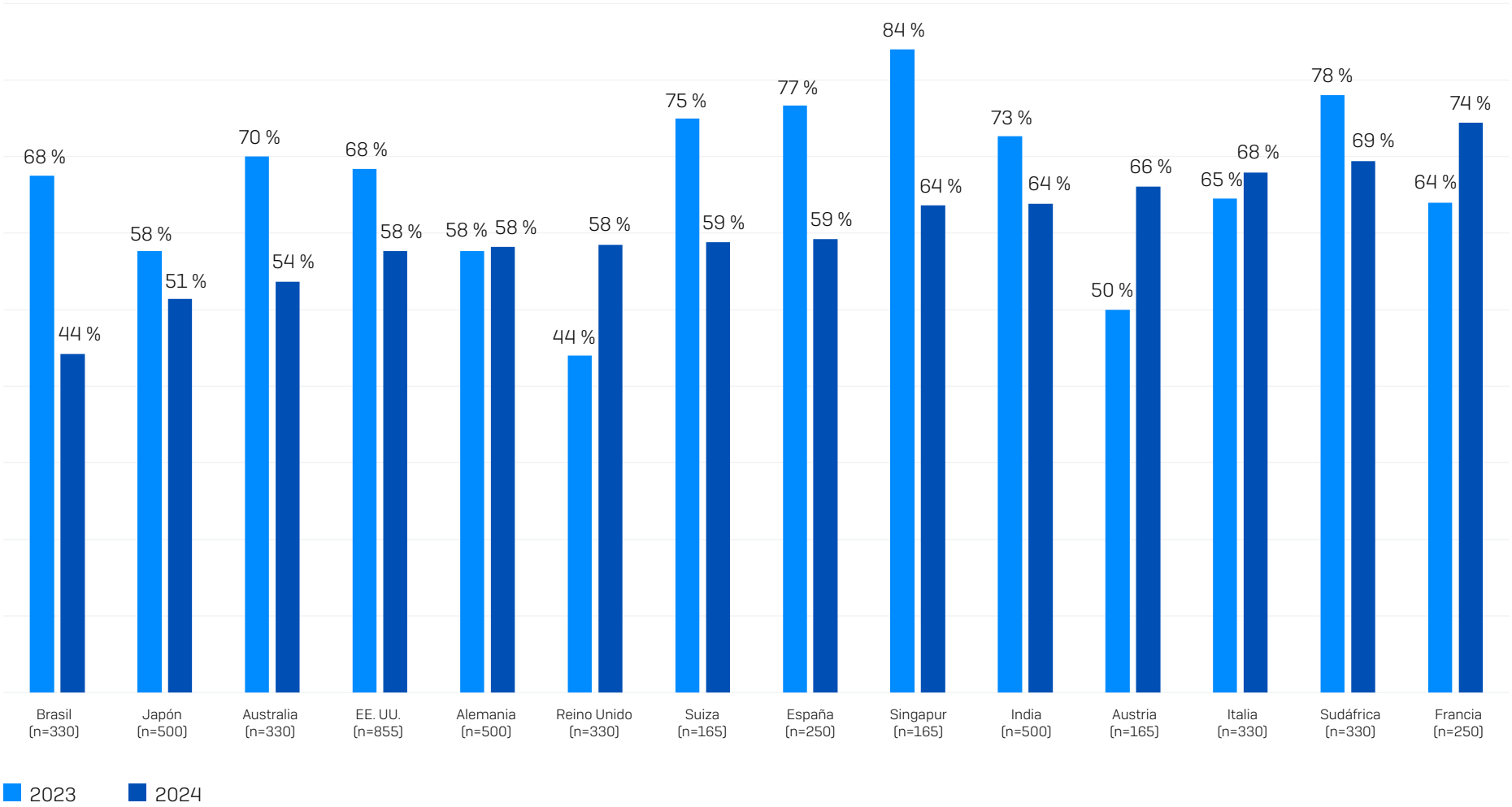
Porcentaje de organizaciones afectadas por el ransomware en el último año



En el último año, ¿se ha visto afectada su organización por el ransomware? Sí. n=5000 (2024), 3000 (2023), 5600 (2022). Números base de 2024, por sector, en el gráfico.

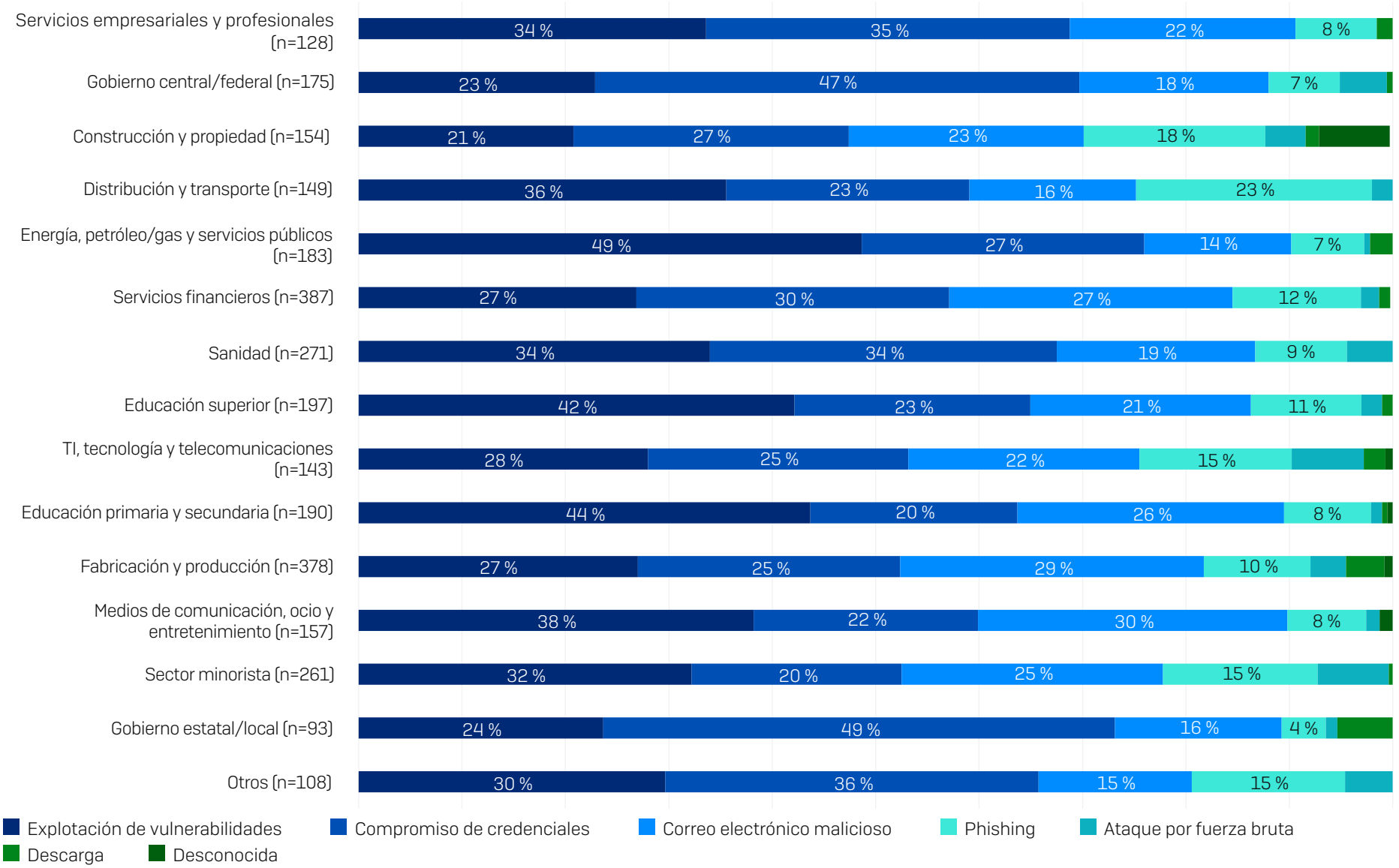
Índice de ataques de ransomware por país

Porcentaje de organizaciones afectadas por el ransomware en el último año



En el último año, ¿se ha visto afectada su organización por el ransomware? Sí. n=5000 (2024), n=3000 (2023). Números base de 2024, por país, en el gráfico.

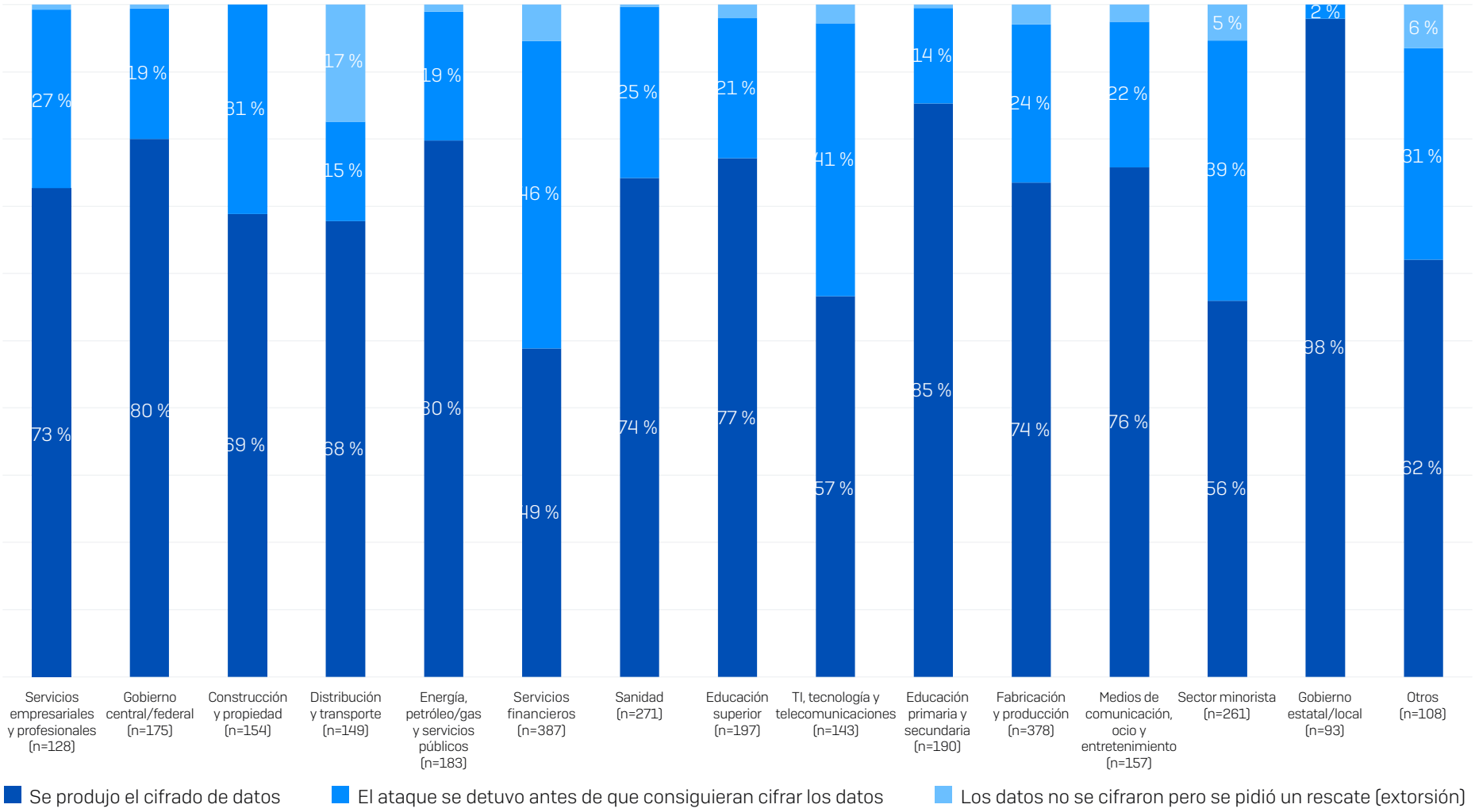
Causas raíz del ataque por sector



¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? n=2974 organizaciones afectadas por el ransomware.

Índice de cifrado de datos por sector

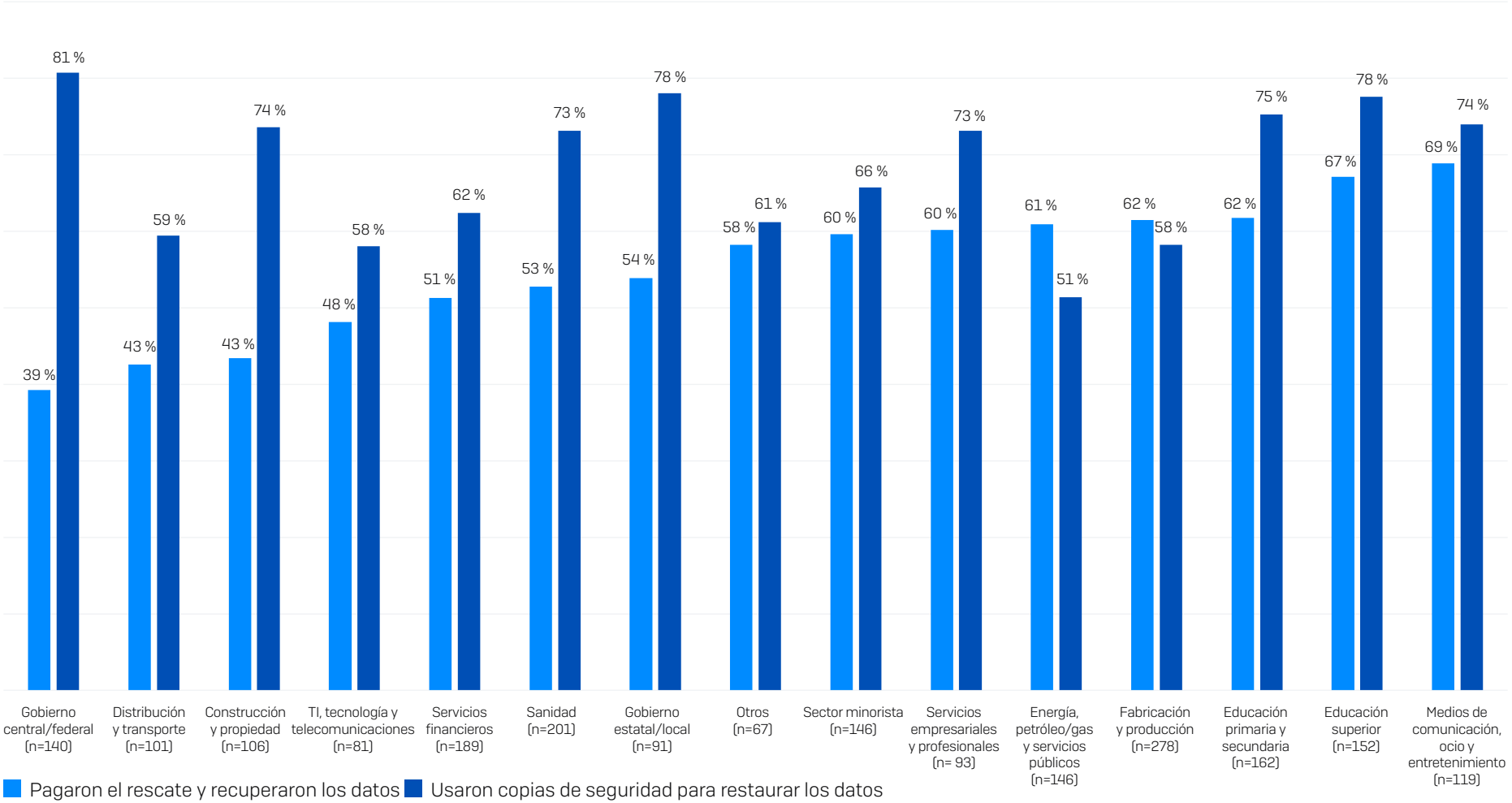
Propensión a sufrir el cifrado de datos en un ataque



¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Número base en la tabla.

Método de recuperación de datos por sector

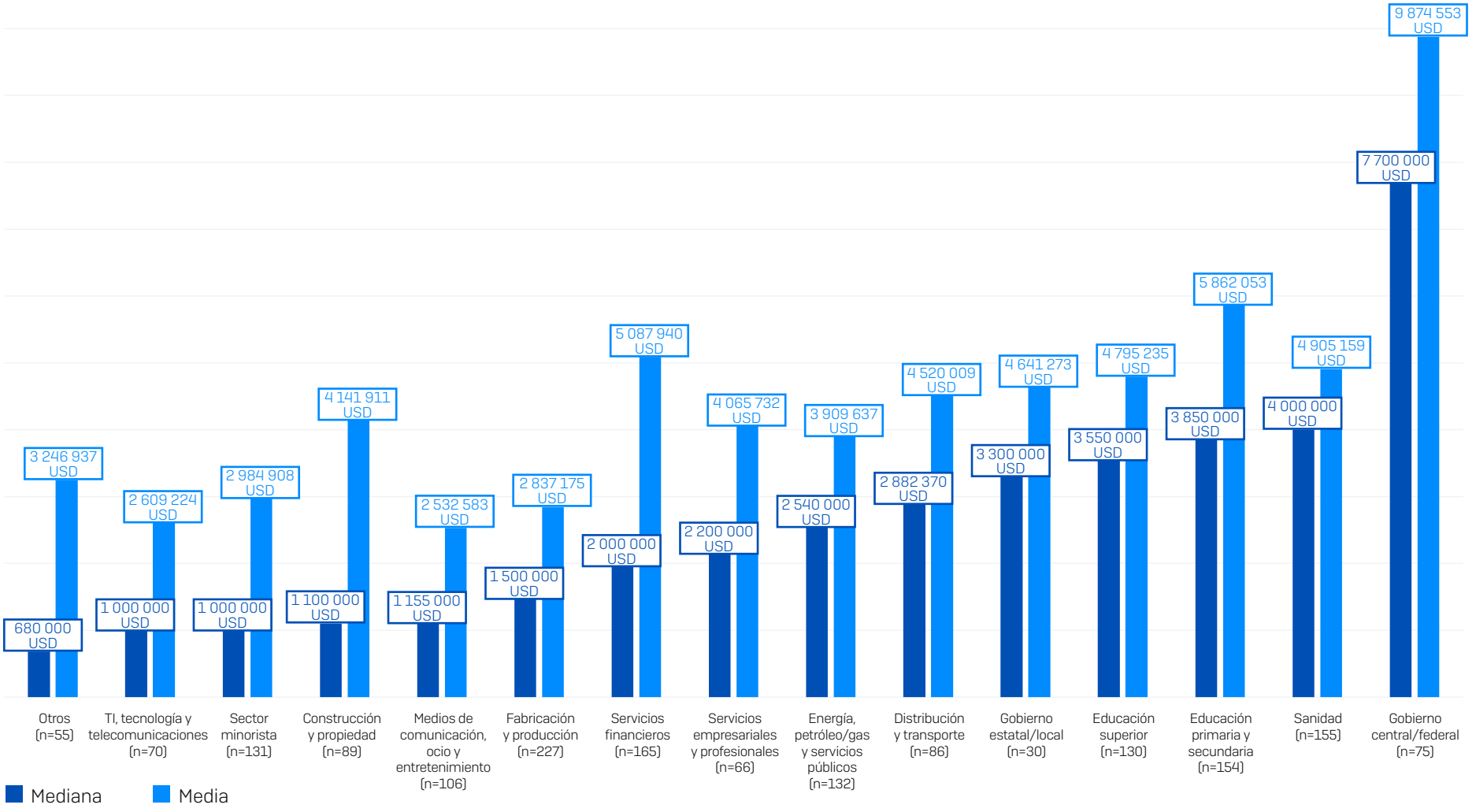
Con qué frecuencia se recuperan los datos usando las copias de seguridad y pagando el rescate



¿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. Ordenados por predisposición a pagar el rescate.

Petición de rescate por sector

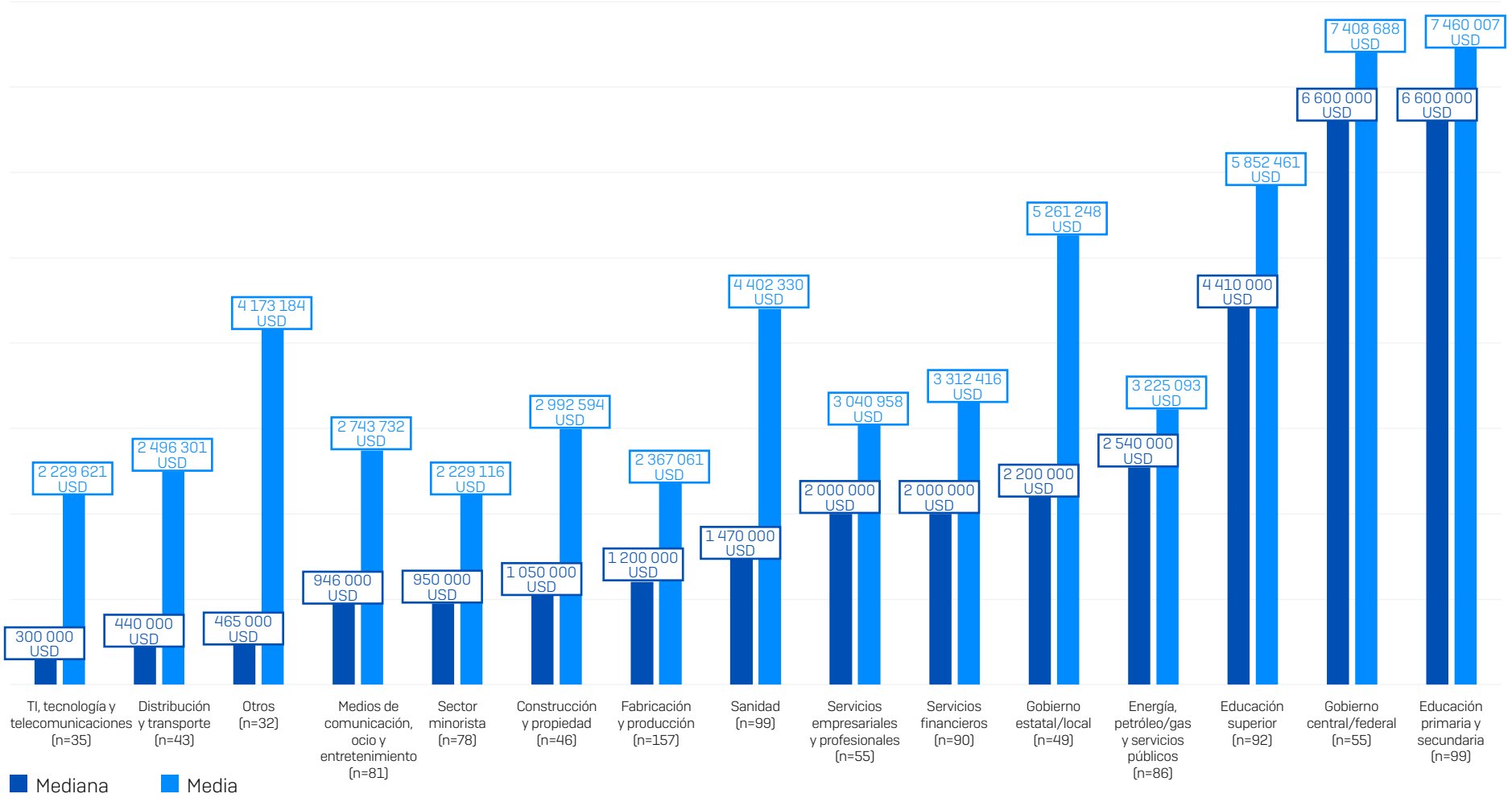
Petición de rescate



¿A cuánto ascendía el rescate exigido por los atacantes? Números base en la tabla. Ordenados por la mediana del rescate exigido.

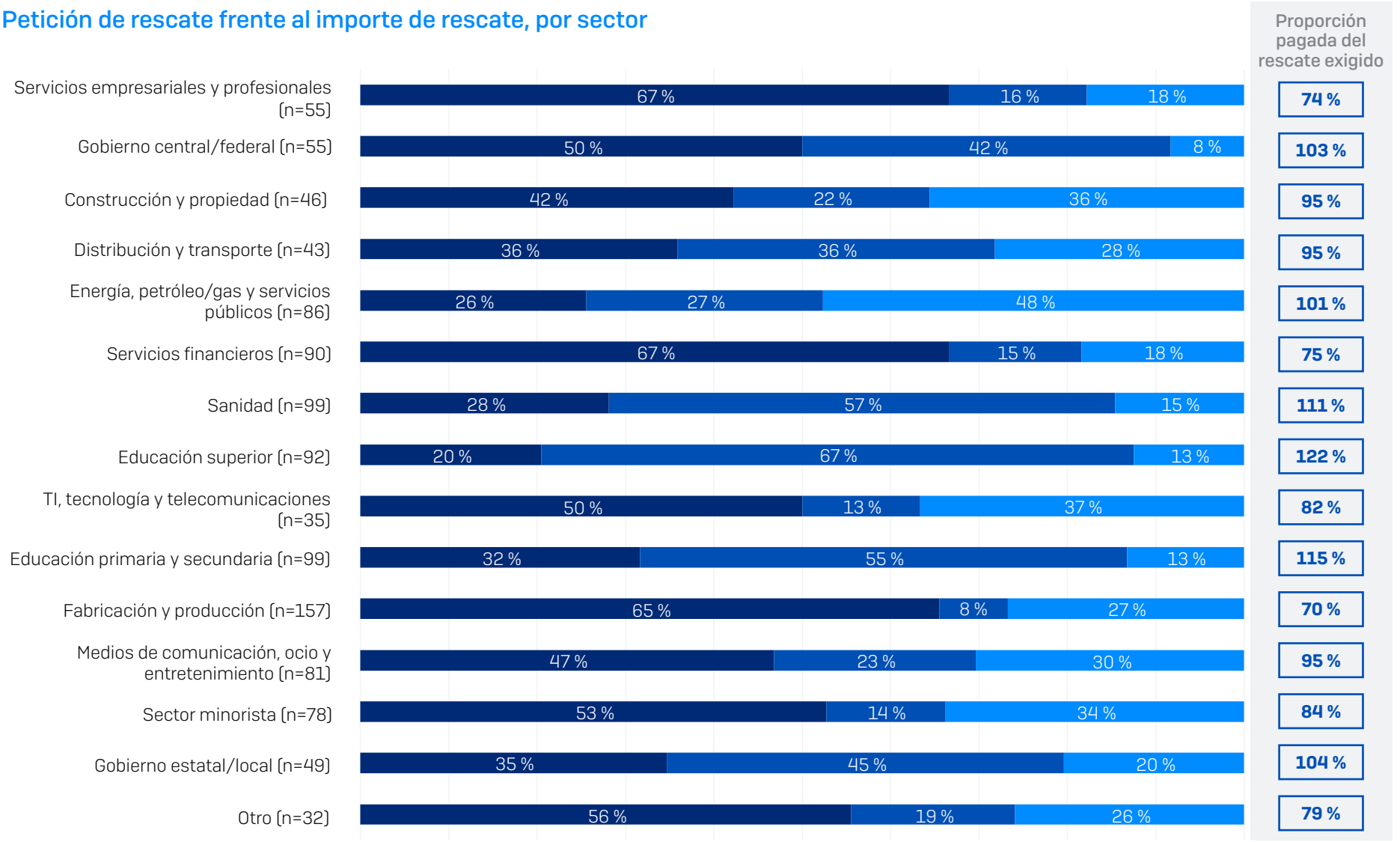
Importe del rescate por sector

Pago de rescate



¿Cuál fue el importe del rescate que pagó su organización a los atacantes? Números base en la tabla. Ordenados por la mediana del pago realizado.

Petición de rescate frente al importe de rescate, por sector



¿A cuánto ascendía el rescate exigido por los atacantes? ¿Cuál fue el importe del rescate que pagó su organización a los atacantes? Números base en la tabla.

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.

2024-04-16 (WP-PC)

SOPHOS