SOPHOS

EL ESTADO DEL RANSOMWARE EN EL SECTOR EDUCATIVO 2025

Resultados de una encuesta independiente realizada a 441 responsables de TI y ciberseguridad del sector educativo en 17 países cuyas organizaciones se vieron afectadas por el ransomware en el último año.

Monográficos de Sophos. Agosto de 2025

Introducción

Le damos la bienvenida a la quinta edición del informe anual de Sophos "El estado del ransomware en el sector educativo", que revela la realidad de esta amenaza en 2025 para las instituciones de educación primaria y secundaria (para estudiantes hasta 18 años) y superior (a partir de 18 años).

En el informe de este año se desvela cómo han evolucionado en el último año las experiencias de las organizaciones educativas con el ransomware, tanto en lo que respecta a las causas como a las consecuencias. También arroja nueva luz sobre cuestiones hasta ahora poco exploradas, como los factores organizativos que exponen a las instituciones educativas a los ataques y el impacto humano de los incidentes en los equipos de TI y ciberseguridad.

En el informe, que se basa en las experiencias reales de 441 responsables de TI y ciberseguridad (243 de instituciones de educación primaria y secundaria y 198 de educación superior afectadas por el ransomware durante el último año), se ofrecen datos clave sobre:

- Por qué sucumben las organizaciones educativas al ransomware.
- Qué ocurre con los datos.
- Peticiones e importes de los rescates.
- El impacto a nivel humano y empresarial 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, 2025. 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 2024.

Acerca de la encuesta

El informe completo se basa en una encuesta independiente y desvinculada de cualquier proveedor realizada a 3400 profesionales de TI/ciberseguridad que trabajan en organizaciones que se vieron afectadas por el ransomware en el último año, entre ellas 441 del sector educativo. El estudio fue encargado por Sophos y realizado por un especialista externo entre enero y marzo de 2025. Todos los encuestados trabajan en organizaciones con entre 100 y 5000 empleados, y se les pidió contestar según sus experiencias en los últimos 12 meses.

Los encuestados proceden de 17 países, lo que garantiza que los resultados de la encuesta reflejen una amplia y diversa gama de experiencias. El informe recoge comparaciones con los resultados de los informes anteriores, lo que nos permite realizar una comparación interanual. Todos los puntos de datos financieros son en dólares estadounidenses (USD).

Principales conclusiones

Por qué sucumben las organizaciones educativas al ransomware

- El **phishing** es la principal causa raíz técnica observada de los ataques de ransomware en la educación primaria y secundaria (22 %), pero los métodos de ataque se distribuyen de manera uniforme entre el phishing, los correos electrónicos maliciosos, la explotación de vulnerabilidades y el compromiso de credenciales. Por el contrario, en la educación superior la **explotación de vulnerabilidades** sigue siendo la causa principal, utilizada en el 35 % de los ataques.
- Al analizar las causas raíz organizativas, para las instituciones de educación superior, las **lagunas de seguridad desconocidas** fueron la causa raíz más frecuente (49 %); para las de educación primaria y secundaria, **la falta de conocimientos especializados y la falta de personal/capacidad** para abordar los ataques fueron las razones más comunes detrás de los ataques (ambas con un 42 %).

Qué ocurre con los datos

- **El índice de cifrado de datos en el sector educativo ha caído a su nivel más bajo en cuatro años:** el 29 % de los ataques en educación primaria y secundaria (el porcentaje más bajo de todos los sectores) y el 58 % en educación superior se saldaron con el cifrado de datos.
- El 26 % de las instituciones de educación primaria y secundaria y el 33 % de las de educación superior cuyos datos fueron cifrados también sufrieron la **exfiltración de datos**.
- El 97 % de las organizaciones educativas a las que les cifraron los datos pudieron recuperarlos.
- El **uso de copias de seguridad para recuperar los datos ha disminuido**: solo el 59 % de las instituciones de educación primaria y secundaria que sufrieron el cifrado de datos utilizaron copias de seguridad, y en el caso de las instituciones de educación superior, el porcentaje fue del 47 %.
- La mitad de las víctimas de educación primaria y secundaria y el 54 % de las de educación superior **pagaron el rescate para recuperar sus datos**.

Los rescates: peticiones e importes

- **La mediana de petición de rescate en el sector educativo se redujo drásticamente:** de 3,85 millones USD a 1,02 millones USD en la educación primaria y secundaria, y de 3,55 millones USD a 697 000 USD en la educación superior, lo que la sitúa entre las peticiones más bajas de todos los sectores analizados.
- **La mediana del importe de rescate pagado también experimentó una fuerte caída.** En la educación primaria y secundaria, los importes desembolsados descendieron de 6,6 millones USD a 800 000 USD, mientras que en la educación superior pasaron de 4,41 millones USD a 463 000 USD. Así, ambos sectores educativos pasaron de estar entre los que más pagaron en 2024 a estar entre los que menos pagaron en 2025.
- En consonancia con la tendencia general, **la proporción del rescate que se paga realmente también disminuyó.** En la educación primaria y secundaria, cayó del 115 % en 2024 al 84 % en 2025, mientras que en la educación superior se registró una caída más pronunciada, del 122 % al 69 %.
- Si se analizan detenidamente las **peticiones de rescate frente a los importes desembolsados**, el 41 % de las instituciones de educación primaria y secundaria pagaron lo que se les pidió inicialmente, el 41 % pagaron menos y el 18 % pagaron más. En el caso de la educación superior, solo el 26 % pagaron lo que se les pidió inicialmente, mientras que el 60 % pagaron menos y el 14 % pagaron más.

El impacto del ransomware en el negocio

- En 2025, **la media de los costes de recuperación en el sector educativo descendió drásticamente.** Los costes de recuperación en la educación superior se desplomaron un 77 %, pasando de 4,02 millones USD en 2024 a 0,90 millones USD (la cifra más baja conjunta), mientras que en la educación primaria y secundaria, a pesar de un descenso del 39 % con respecto a los 3,76 millones USD del año anterior, se registró el coste de recuperación más alto de todos los sectores: 2,28 millones USD.
- **Las organizaciones educativas se recuperan cada vez más rápido de los ataques**. La mitad de las instituciones de educación primaria y secundaria y el 59 % de las de educación superior se recuperaron completamente en una semana (ambos porcentajes superan el 30 % registrado en 2024).

El impacto del ransomware a nivel humano

Todas las organizaciones educativas (tanto de educación primaria y secundaria como de educación superior) cuyos datos fueron cifrados señalaron que el equipo de TI/ciberseguridad se vio **directamente afectado**:

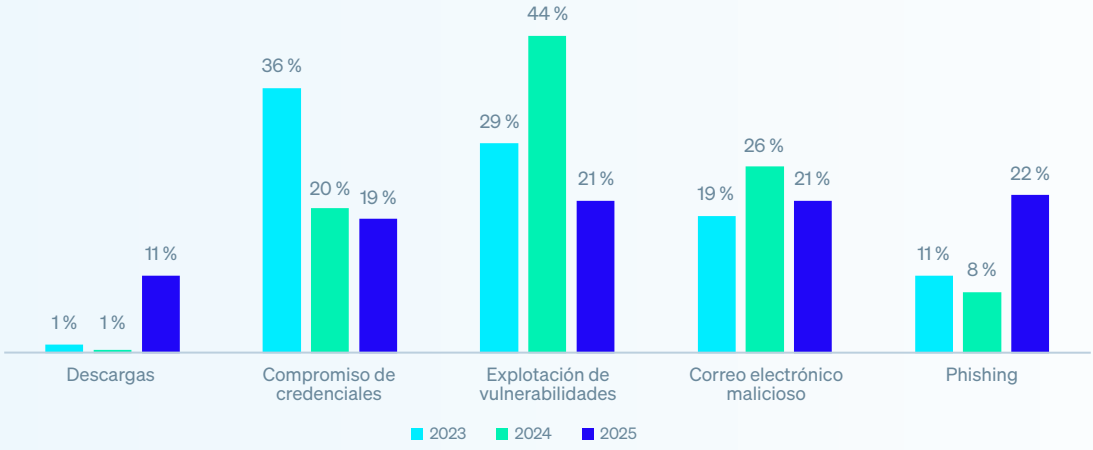
- El 41 % de los equipos de TI/ciberseguridad del sector educativo manifestaron un **aumento de la ansiedad o el estrés** ante futuros ataques.
- El 40 % aseguró que ha **aumentado la presión** por parte de los cargos directivos, pero el 31 % afirmó haber recibido un **mayor reconocimiento**.
- El 38 % mencionó tanto un **cambio en las prioridades/enfoque del equipo** como un **aumento continuo** de la carga de trabajo como factores que afectan a su equipo de TI o ciberseguridad.
- El 37 % registró cambios en la **estructura del equipo o de la organización** como consecuencia del incidente.
- Un tercio (34 %) afirmó que el equipo tenía **sentimiento de culpa** por no haber detenido el ataque a tiempo.
- El 31 % de los equipos se vio afectado por las **bajas del personal** por **problemas de estrés/salud mental** relacionados con el ataque.
- En una cuarta parte de los casos, **se sustituyó a los responsables** del equipo como consecuencia del ataque.

Por qué sucumben las organizaciones educativas al ransomware

Causa raíz técnica de los ataques en el sector educativo

La principal causa raíz técnica de los ataques varía entre las instituciones de educación primaria y secundaria y las de educación superior. Por primera vez en nuestra investigación, el **phishing** es la primera causa raíz de los ataques a las instituciones de educación primaria y secundaria, utilizada en el 22 % de los incidentes. Sin embargo, los cuatro vectores principales (phishing, correos electrónicos maliciosos, explotación de vulnerabilidades y compromiso de credenciales) distan entre sí menos de un 3 %, una distribución excepcionalmente uniforme que no se observa en otros sectores.

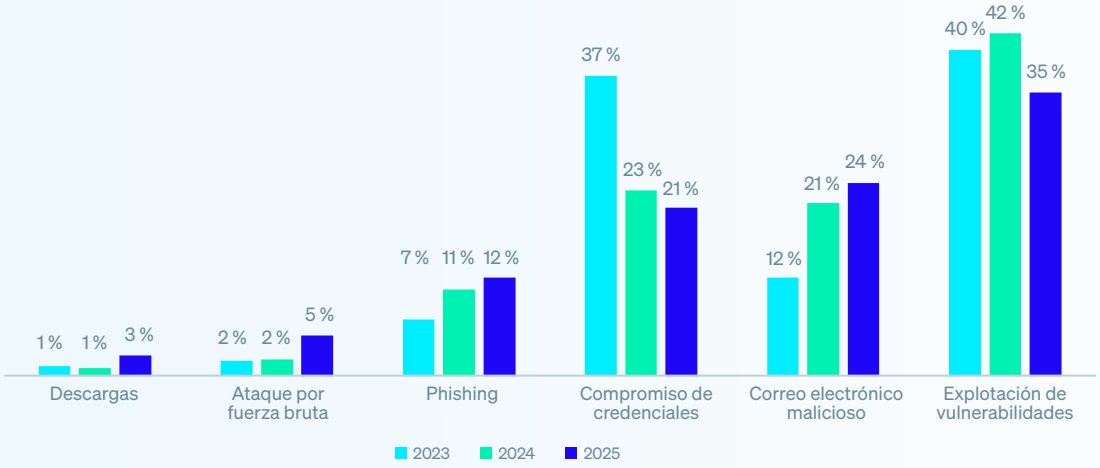
Gráfico 1: causa raíz técnica de los ataques de ransomware en la educación primaria y secundaria 2023 - 2025



¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? Sí. n=243 (2025), 189 (2024), 159 (2023).

Por otro lado, por tercer año consecutivo, las organizaciones de educación superior afectadas señalaron la **explotación de vulnerabilidades** como la causa raíz más común de los incidentes de ransomware: se utilizó para infiltrarse en las instituciones en el 35 % de los ataques, cifra que coincide con la mayoría de los sectores encuestados. Los correos electrónicos maliciosos son el segundo vector de ataque más común, ya que el porcentaje de ataques que utilizaron este método aumentó del 21 % en 2024 al 24 % en 2025. Le sigue muy de cerca el compromiso de credenciales, notificado por el 21 % de las instituciones de educación superior.

Gráfico 2: causa raíz técnica de los ataques de ransomware en la educación superior 2023 - 2025

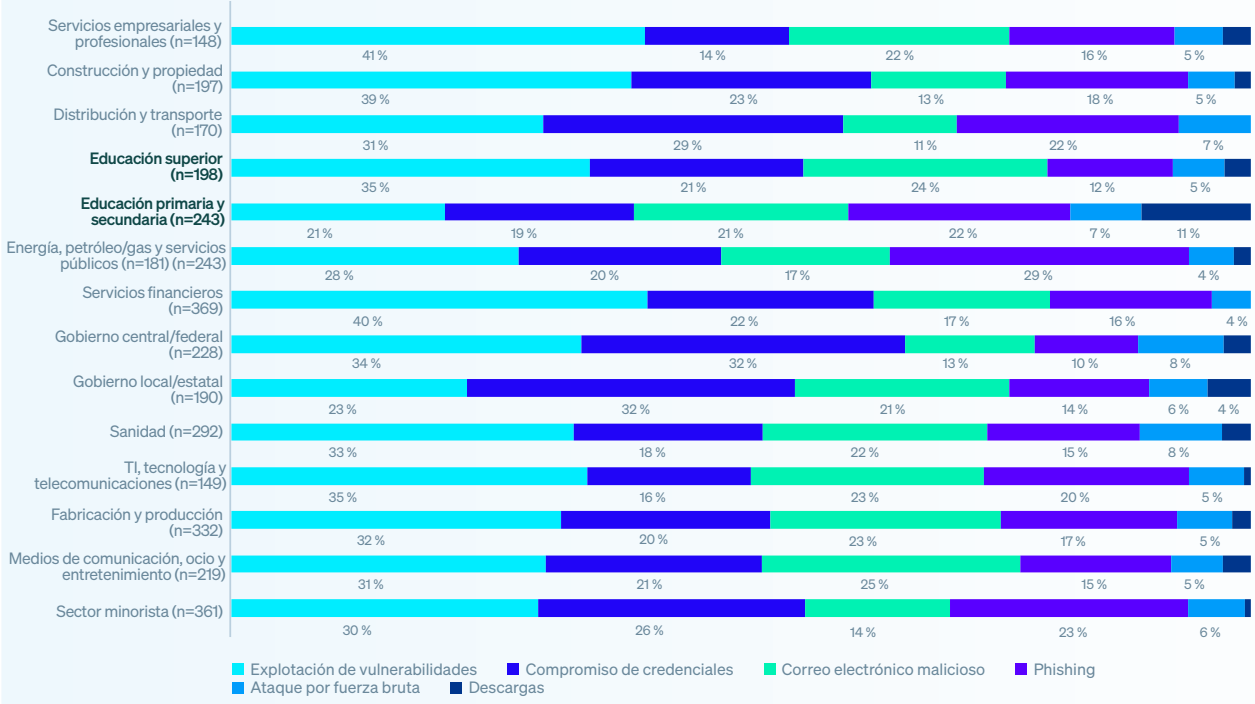


¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? Sí. n=196 (2025), 197 (2024), 156 (2023).

La investigación revela que, a pesar de que las causas raíz varían en función del sector, **la explotación de vulnerabilidades es un vector importante** en casi todos ellos. Excepciones importantes:

- El phishing fue la causa raíz más común citada tanto por instituciones de educación primaria y secundaria (22 %) como por proveedores de energía, petróleo/gas y servicios públicos (29 %).
- El **compromiso de credenciales** fue el vector de ataque percibido más común por las organizaciones de gobiernos estatales y locales, representando casi un tercio de los incidentes (32 %).

Gráfico 3: causa raíz técnica de los ataques de ransomware dividida por tamaño de la organización

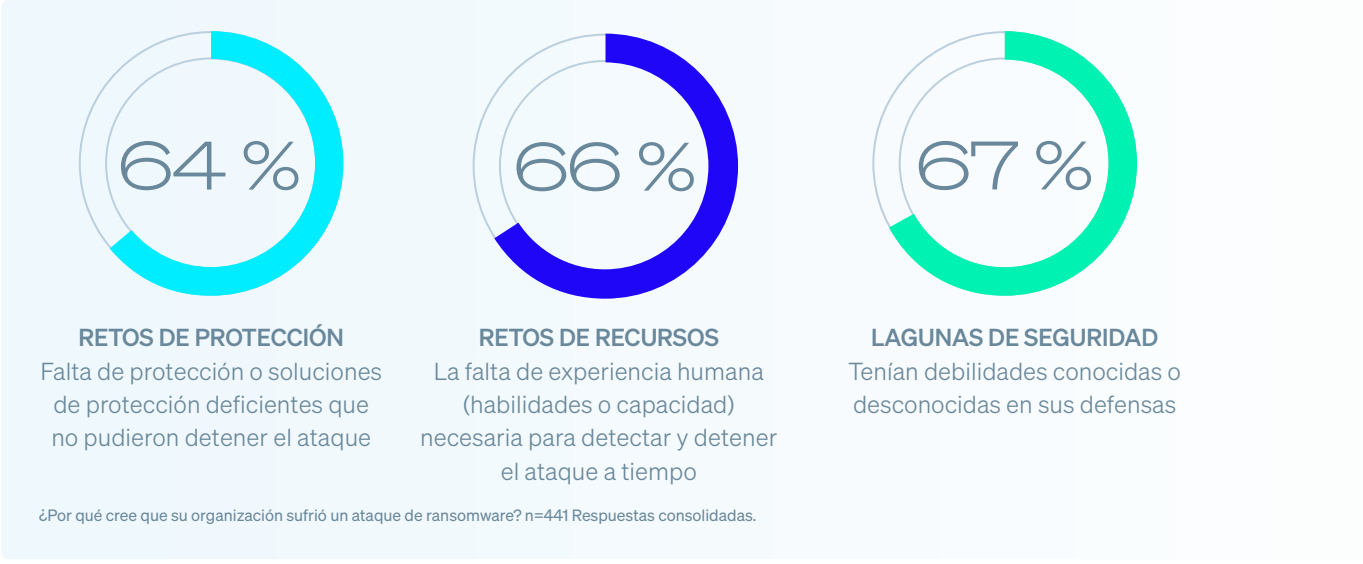


¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año? - Sí. Números base en la tabla.

Causa raíz organizativa de los incidentes en el sector educativo

Por primera vez, el informe de este año analiza los factores organizativos que expusieron a las instituciones educativas a los ataques. Revela que las víctimas del sector educativo suelen enfrentarse a múltiples retos organizativos: de media, los encuestados citaron tres factores que contribuyeron a sufrir un ataque de ransomware.

En general, las causas raíz organizativas se distribuyen de manera bastante uniforme entre problemas de protección (64 %), retos planteados por la dotación de recursos (66 %) y lagunas de seguridad (67 %).

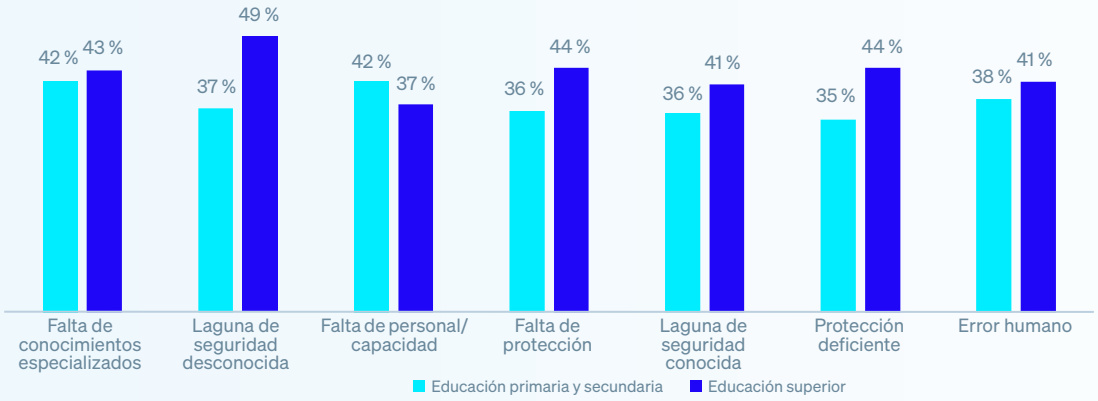


Sin embargo, la distribución entre la educación primaria y secundaria y la educación superior pone de manifiesto variaciones, especialmente entre las instituciones de educación primaria y secundaria, que suelen citar con mayor frecuencia las limitaciones de recursos como la principal causa raíz organizativa del ataque, por delante de las lagunas de seguridad.

Al profundizar en las causas raíz organizativas **individuales**, tanto la **falta de conocimientos especializados** para detectar y detener el ataque a tiempo como la **falta de personal/capacidad** para supervisar los sistemas en el momento del ataque fueron las razones más comunes detrás de los ataques de las instituciones de educación primaria y secundaria, según el 42 % de las víctimas en ambos casos. A esto le siguen los **errores humanos** (es decir, los equipos cometieron un error o no siguieron los procesos correctamente), que contribuyeron al 38 % de los ataques.

En el caso de las instituciones de educación superior, las **lagunas de seguridad desconocidas** (es decir, debilidades en las defensas que la organización desconocía) son la razón individual más común, mencionada por casi la mitad (49 %) de los encuestados, el porcentaje más alto atribuido a esta causa de todos los sectores analizados. A esta le siguen la **protección deficiente** (es decir, sus productos y servicios de ciberseguridad no pudieron detener el ataque) y la **falta de protección** (es decir, no contaban con los productos y servicios de ciberseguridad necesarios), que contribuyeron al 44 % de los ataques en ambos casos.

Gráfico 4: causa raíz organizativa de los ataques de ransomware a instituciones educativas



¿Por qué cree que su organización sufrió un ataque de ransomware? n=243 (educación primaria y secundaria), 198 (educación superior)

Causa raíz organizativa según el sector

La causa organizativa más común también varía según el sector, lo que pone de manifiesto los desafíos tan diferentes que afrontan las empresas. Cabe destacar que ningún sector señaló el error humano como la razón más común detrás del ataque de ransomware.

Gráfico 5: principales causas raíz organizativas de los ataques de ransomware por sector

FALTA DE CONOCIMIENTOS ESPECIALIZADOS	LAGUNA DE SEGURIDAD DESCONOCIDA	FALTA DE PERSONAL/ CAPACIDAD	FALTA DE PROTECCIÓN	LAGUNA DE SEGURIDAD CONOCIDA	PROTECCIÓN DEFICIENTE
No teníamos las habilidades o conocimientos necesarios para detectar y detener el ataque a tiempo	Teníamos un punto débil en nuestras defensas que desconocíamos	No teníamos suficientes expertos en ciberseguridad que supervisaran nuestros sistemas en el momento del ataque	No contábamos con los productos y servicios de ciberseguridad necesarios	Teníamos puntos débiles en nuestras defensas que ya conocíamos pero que no habíamos solucionado	Nuestros productos y servicios de ciberseguridad no fueron capaces de detener el ataque
Energía, petróleo/ gas y servicios públicos (43 %)	**Educación superior (más de 18 años) (49 %)**	**Educación primaria y secundaria (42 %) ***	Servicios financieros, incl. seguros (44 %) *	Gobierno central/ federal (45 %)	Medios de comunicación, ocio y entretenimiento (44 %)
Educación primaria y secundaria (42 %) *	Servicios empresariales y profesionales (46 %)	Sanidad (42 %)	Gobierno local/ estatal (40 %)	TI, tecnología y telecomunicaciones (42 %)	Distribución y transporte (41 %)
Fabricación y producción (42 %)	Comercio minorista (46 %)			Construcción y propiedad (41 %) *	
Construcción y propiedad (41 %) *	Servicios financieros, incl. seguros (44 %) *				

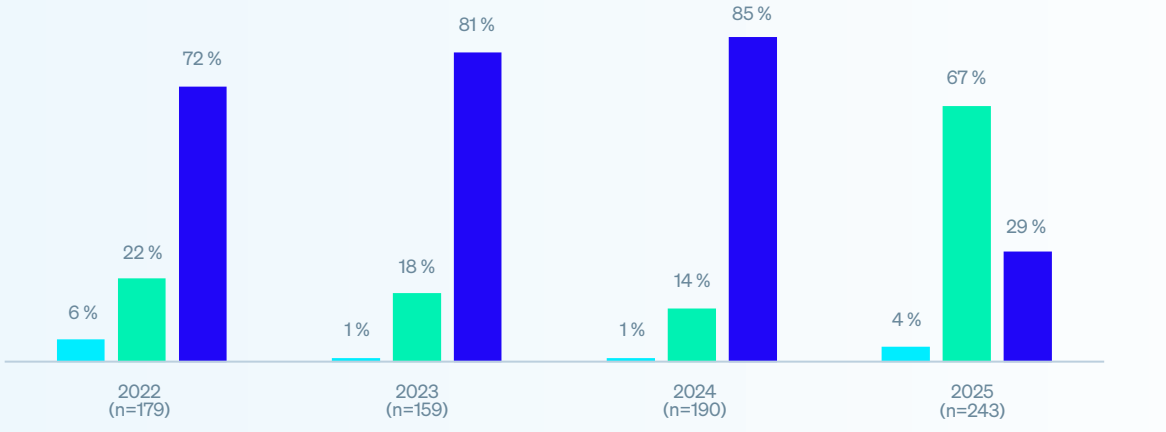
¿Por qué cree que su organización sufrió un ataque de ransomware? n=3400. Dividido por sector.
* indica dos causas raíz principales conjuntas

Qué ocurre con los datos

Cifrado de datos en el sector educativo

Es alentador que **los índices de cifrado de datos en el sector educativo hayan disminuido**. En la educación primaria y secundaria, solo el 29 % de los ataques derivaron en el cifrado de datos, lo que supone el mínimo en cuatro años y el índice más bajo registrado en todos los sectores analizados. En consonancia con ese índice de cifrado a la baja, el índice de ataques detenidos con éxito antes del cifrado se disparó del 14 % en 2024 al 67 % en 2025, de nuevo el más alto de todos los sectores y muy por encima de la media intersectorial del 44 %. Esto indica que, actualmente, las organizaciones de educación primaria y secundaria son más capaces que nunca de detectar y bloquear los ataques de ransomware antes de que causen daños.

Gráfico 6: índice de cifrado de datos en los ataques de ransomware a instituciones educativas 2022 - 2025

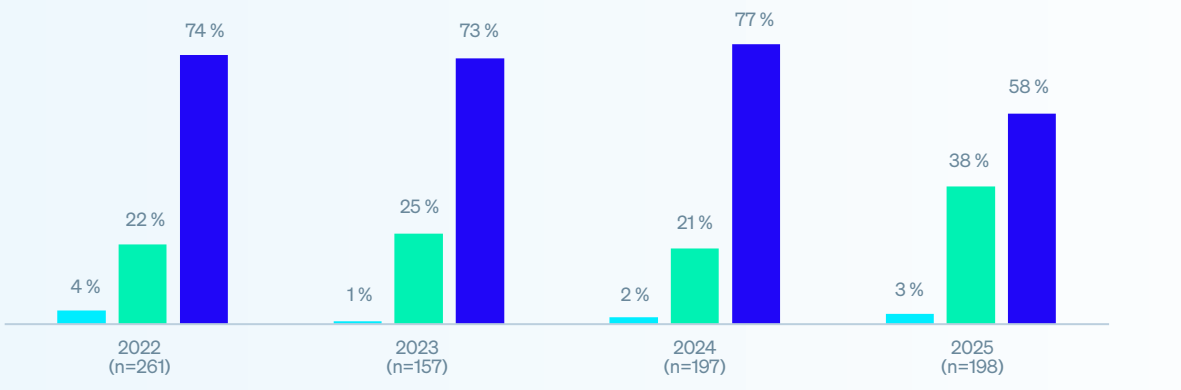


¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Números base en la tabla.

Las instituciones de educación superior mantuvieron su tendencia a la baja en cuanto al cifrado de datos: el índice cayó al 58 %, el nivel más bajo en cuatro años, frente al 77 % registrado en 2024. Aunque se trata de un dato prometedor, sigue estando por encima de la media intersectorial del 50 %.

Como dato positivo, **la proporción de ataques detenidos antes del cifrado casi se duplicó**, pasando del 21 % al 38 % (aunque por debajo de la media intersectorial del 44 %). Esto apunta a una mejora de las capacidades defensivas, pero también pone de relieve que las organizaciones de educación superior siguen estando expuestas, probablemente debido a la complejidad de sus entornos de TI, a su infraestructura heredada y a sus amplias bases de usuarios descentralizadas.

Gráfico 7: índice de cifrado de datos en los ataques de ransomware a instituciones de educación superior 2022 - 2025



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

Robo de datos

Los adversarios no solo cifran los datos, sino que también los roban. Las instituciones de educación superior son las que corren un mayor riesgo: representan el 19 % de todas las víctimas, y el 33 % de las instituciones cuyos datos fueron cifrados denunciaron también el robo de datos, en comparación con solo el 7 % y el 26 % en la educación primaria y secundaria. Probablemente, esto se deba a que los datos son más valiosos, los sistemas están descentralizados y el acceso externo es más amplio, lo que es típico de la educación superior y dificulta la detección y el control. La tendencia también coincide con los resultados de la prevención: las instituciones de educación primaria y secundaria detuvieron el 67 % de los ataques antes del cifrado, una cifra considerablemente superior a la de la educación superior, que fue del 38 %.

Ataques de tipo extorsión

Como se muestra en los gráficos 6 y 7, el porcentaje de organizaciones educativas que no sufrieron el cifrado de datos, pero que se les pidió un rescate de todas formas (extorsión), ha aumentado ligeramente a lo largo del año (pasando del 1 % en 2024 al 4 % en el caso de la educación primaria y secundaria y del 2 % en 2024 al 3 % en el de la educación superior), lo que sugiere un cambio en las tácticas de los atacantes a medida que mejoran las defensas.

En general, las instituciones de educación primaria y secundaria son las que mejor pueden prevenir con éxito las consecuencias de un ataque de ransomware, es decir, impedir que se cifren los datos, evitar la exfiltración de datos y evitar ser objeto de extorsión. Esto sugiere que este tipo de instituciones están demostrando ser sorprendentemente eficaces en la detección e intervención tempranas, incluso con presupuestos limitados.

Recuperación de los datos cifrados en el sector educativo

El 97 % de las organizaciones educativas a las que les cifraron los datos pudieron recuperarlos.

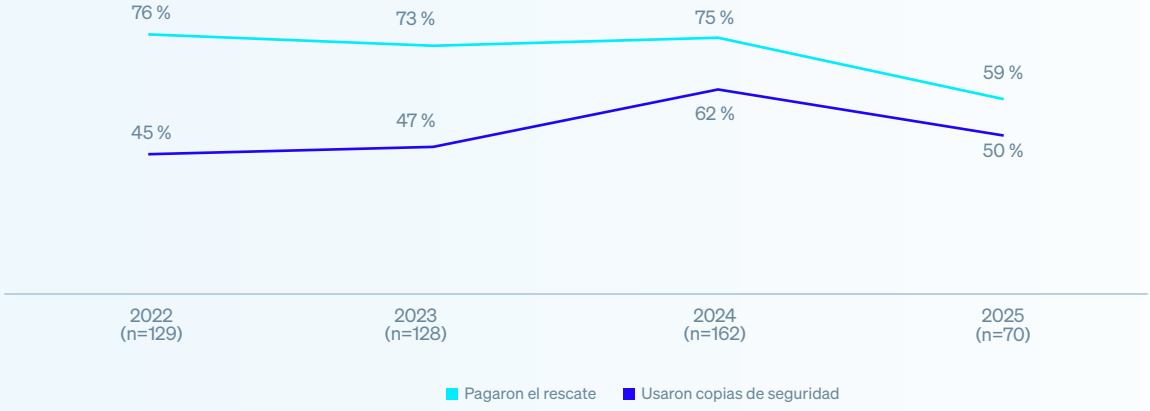
El **uso de copias de seguridad** por parte de las instituciones de educación primaria y secundaria para restaurar los datos alcanzó su mínimo en cuatro años, con un 59 %, lo que supone un descenso considerable con respecto al 75 % registrado en 2024. A pesar de ello, la educación primaria y secundaria sigue estando entre los cuatro sectores que más utilizan las copias de seguridad para restaurar los datos en la encuesta de este año.

La mitad de las organizaciones de educación primaria y secundaria **pagaron el rescate y recuperaron sus datos**, en línea con la media intersectorial del 49 %. Aunque se trata de una reducción notable con respecto al 62 % del año pasado, sigue siendo el segundo índice más alto de pago de rescates realizados por organizaciones de educación primaria y secundaria en los últimos cuatro años.

La reducción de la brecha entre las instituciones de educación primaria y secundaria que pagan el rescate para recuperar los datos y las que utilizan copias de seguridad para restaurarlos sugiere una creciente dependencia de métodos de recuperación múltiples o alternativos.

Como prueba de ello, comprobamos que más de un tercio (34 %) de las instituciones de educación primaria y secundaria cuyos datos fueron cifrados afirmaron **haber utilizado más de un método para restaurarlos**.

Gráfico 8: recuperación de los datos cifrados en la educación primaria y secundaria 2022 - 2025



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

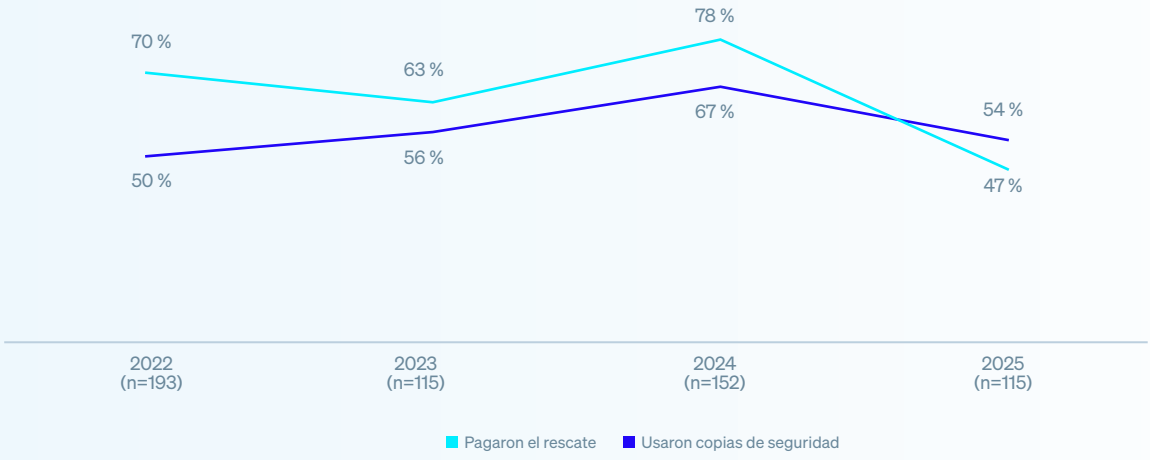
Entre las instituciones de educación superior, solo el 47 % utilizó **copias de seguridad para restaurar los datos**, un fuerte descenso con respecto al 78 % registrado en 2024, lo que sitúa al sector entre los tres últimos en cuanto al uso de copias de seguridad. Esto puede deberse a las infraestructuras de TI descentralizadas, los entornos de datos complejos, los sistemas heredados y las prácticas de copia de seguridad incoherentes que suelen caracterizar a las instituciones de educación superior.

El 54 % de las organizaciones de educación superior **pagaron el rescate y recuperaron sus datos**, lo que supone un porcentaje ligeramente superior al 49 % de la media intersectorial, pero un bienvenido descenso con respecto al 78 % registrado en 2024.

Al igual que ocurre en las organizaciones de educación primaria y secundaria, la reducción de la brecha entre las instituciones de educación superior que pagan el rescate para recuperar los datos y las que utilizan copias de seguridad para restaurarlos sugiere una creciente dependencia de métodos de recuperación múltiples o alternativos.

Como prueba de ello, constatamos que el 38 % de las instituciones de educación superior que sufrieron el cifrado de datos afirmaron **utilizar más de un método para restaurar sus datos**, lo que sitúa al sector entre los tres más propensos a esta práctica.

Gráfico 9: recuperación de los datos cifrados en la educación superior 2022 - 2025



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

Rescates

Peticiones de rescate para las instituciones educativas

Durante el último año, la mediana de petición de rescate exigido a las instituciones educativas se redujo considerablemente. La petición de rescate en el caso de la educación primaria y secundaria descendió un 74 %, pasando de 3,85 millones USD en 2024 a 1,02 millones USD, mientras que la petición de rescate en la educación superior se redujo de 3,55 millones USD en 2024 a solo 697 000 USD, uno de los rescates exigidos más bajos registrados en todos los sectores analizados.

	2024	2025
Educación primaria y secundaria	3,85 MUSD (n=154)	1,02 MUSD (n=69)
Educación superior	3,55 MUSD (n=130)	697 000 USD (n=112)

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

La media intersectorial siguió una tendencia similar: descendió en un tercio (34 %) hasta alcanzar los 1,32 millones USD en 2025, frente a los 2 millones USD de 2024.

La disminución de las peticiones de rescate a instituciones educativas se debe en gran medida a una reducción considerable de las peticiones de alto valor. Las instituciones de educación primaria y secundaria registraron un descenso del 86 % en las peticiones de 5 millones USD o más, mientras que las instituciones de educación superior registraron una caída del 34 % en las peticiones de 1 millón USD o más. Esto parece indicar que los atacantes podrían estar cambiando de estrategia y preferir pagos más pequeños e inmediatos en lugar de grandes cantidades.

Pagos de rescates por parte de las instituciones educativas

Al igual que los rescates exigidos, **los pagos de rescate medios (mediana)** realizados tanto por instituciones de educación superior como por instituciones de educación primaria y secundaria **disminuyeron considerablemente** durante el último año: pasaron de estar entre los más altos en 2024 a estar entre los más bajos en 2025, lo que indica que estas organizaciones podrían estar rechazando de manera más contundente las peticiones abusivas.

La mediana del rescate pagado por las instituciones de educación primaria y secundaria se desplomó un 88 %, pasando de 6,60 millones USD en 2024 a 800 000 USD. Por otro lado, los pagos realizados por las instituciones de educación superior cayeron de 4,41 millones USD en 2024 a solo 463 000 USD, situándose entre los cuatro importes más bajos registrados en la encuesta de este año.

	2024	2025
Educación primaria y secundaria	6,60 MUSD (n=99)	800 000 USD (n=35)
Educación superior	4,41 MUSD (n=92)	463 000 USD (n=65)

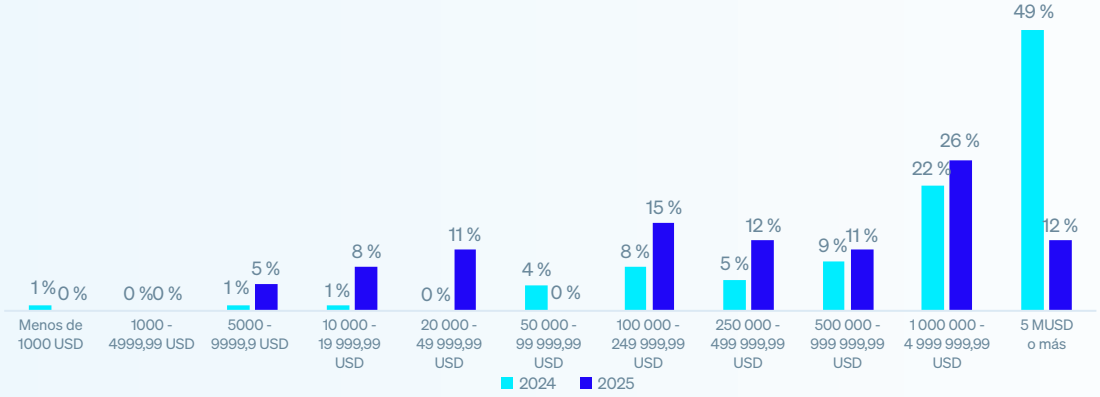
¿A cuánto ascendió el rescate que pagó su organización a los atacantes? Números base en la tabla.

La disminución de los importes de rescate pagados por las instituciones educativas se debe en gran medida a una reducción considerable de los pagos de alto valor, de 5 millones USD o más, registrándose una disminución del 89 % en las instituciones de educación primaria y secundaria y del 75 % en las de educación superior.

Gráfico 10: importe de los rescates en la educación primaria y secundaria | Distribución por bandas

¿Cuál fue el importe de rescate que pagó su organización a los atacantes? n=35 (2025), 99 (2024)

Gráfico 11: importe de los rescates en la educación superior | Distribución por bandas

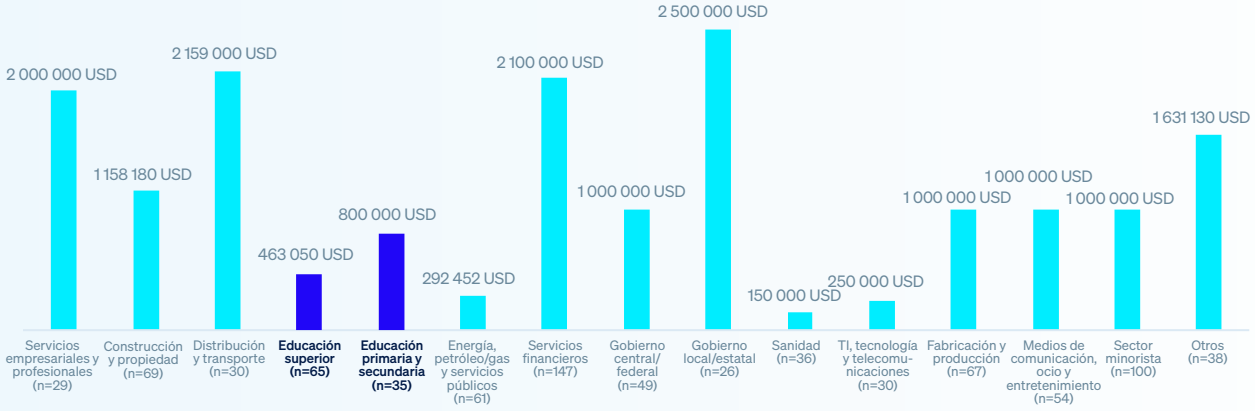


¿A cuánto ascendió el rescate que pagó su organización a los atacantes? n=65 (2025), 92 (2024)

Importes de los rescates por sector

Los importes de los rescates variaron considerablemente dependiendo del sector, y las organizaciones de gobierno estatales y locales pagaron la cantidad media más alta a los atacantes: 2,5 millones USD. Esto puede deberse a las presiones de los servicios críticos, la limitada resiliencia cibernética y el hecho de que los atacantes se aprovechen de su urgencia por recuperarse rápidamente. En cambio, los proveedores de atención sanitaria pagaron el importe más bajo, tan solo 150 000 USD.

Gráfico 13: Importes de los rescates por sector

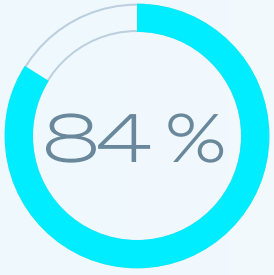


¿A cuánto ascendió el rescate que pagó su organización a los atacantes? Números base en la tabla.
Nota: debido a los bajos números base en los sectores de servicios empresariales y de gobierno local/estatal, los resultados deben considerarse meramente orientativos.

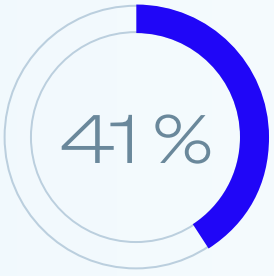
Comparativa entre los importes desembolsados por las instituciones educativas y la petición inicial

34 instituciones de educación primaria y secundaria que pagaron el rescate compartieron tanto la petición inicial como la cantidad pagada realmente, lo que puso de manifiesto que pagaron, de media, el 84 % de la petición de rescate inicial, un bienvenido descenso con respecto al 115 % registrado en 2024. En general, el 41 % pagó menos de lo que se les solicitaba inicialmente (muy por debajo de la media intersectorial del 53 %), el 18 % pagó más y el 41 % igualó la petición inicial.

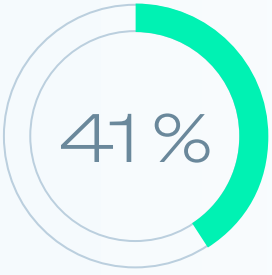
34 instituciones de educación primaria y secundaria que pagaron el rescate revelaron la petición inicial y la cantidad pagada realmente, lo que demuestra que:



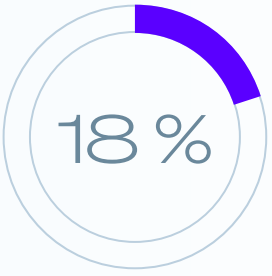
porcentaje **que se pagó** de la petición de rescate, de media



de los importes de rescate pagados fueron **inferiores** a la petición inicial



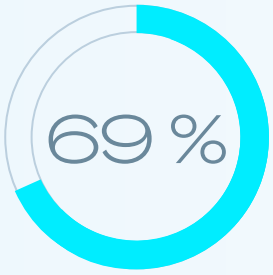
de los importes de rescate pagados **coincidieron** con la petición inicial



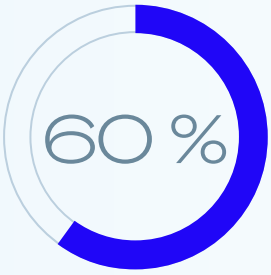
de los importes de rescate pagados fueron **superiores** a la petición inicial

65 organizaciones de educación superior que pagaron el rescate compartieron tanto la petición inicial como la cantidad pagada realmente, lo que puso de manifiesto que pagaron, de media, solo el 69 % de la petición de rescate inicial, lo que supone una caída considerable con respecto al 122 % registrado en 2024 y el índice más bajo registrado en la encuesta de este año. En general, el 60 % pagó menos de lo que se les solicitaba inicialmente (un porcentaje notablemente superior a la media intersectorial del 53 %), el 14 % pagó más y el 26 % igualó la petición inicial.

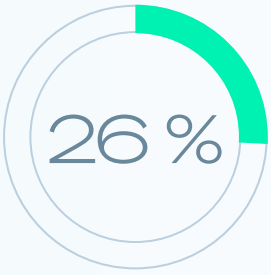
65 instituciones de educación superior que pagaron el rescate revelaron la petición inicial y la cantidad pagada realmente, lo que demuestra que:



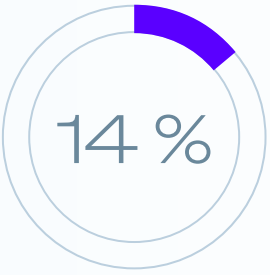
porcentaje **que se pagó** de la petición de rescate, de media



de los importes de rescate pagados fueron **inferiores** a la petición inicial



de los importes de rescate pagados **coincidieron** con la petición inicial



de los importes de rescate pagados fueron **superiores** a la petición inicial

Por qué la mayoría de los importes de rescate pagados por las organizaciones educativas difieren del importe exigido inicialmente

Este año, por primera vez, hemos analizado por qué algunas instituciones educativas pagan menos de lo exigido inicialmente, lo que arroja nueva luz sobre un aspecto crítico a la hora de hacer frente a un ataque de ransomware.

Según revelaron 15 instituciones de **educación primaria y secundaria*** que **pagaron menos** que la petición inicial:

- 67 %: Los atacantes redujeron su petición para animarnos a pagar (el porcentaje más alto en este sentido en la encuesta de este año).
- 60 %: Nos hicieron un descuento por pagar el rescate rápido.
- 53 %: Los adversarios redujeron su petición inicial debido a presiones externas (por ejemplo, de los medios de comunicación o de las fuerzas de seguridad).
- 53 %: Un tercero negoció una cantidad inferior con los atacantes.
- 33 %: Negociamos una cantidad inferior con los atacantes.

**Importante: debido al bajo número base de organizaciones, los resultados deben considerarse meramente orientativos.*

39 organizaciones de **educación superior** que **pagaron menos** que la petición inicial explicaron cómo consiguieron reducir el importe del rescate:

- 59 %: Negociamos una cantidad menor con los atacantes (el porcentaje más alto registrado en este sentido en la encuesta de este año).
- 46 %: Nos hicieron un descuento por pagar el rescate rápido.
- 44 %: Los atacantes rebajaron su petición para animarnos a pagar.
- 41 %: Un tercero negoció una cantidad inferior con los atacantes.
- 38 %: Los adversarios redujeron su petición inicial debido a presiones externas (por ejemplo, de los medios de comunicación o de las fuerzas de seguridad).

Entre las instituciones de educación superior y las de educación primaria y secundaria, las razones por las que pagaron menos de lo exigido inicialmente varían considerablemente. En el caso de las instituciones de educación primaria y secundaria, el motivo principal fue que **los atacantes rebajaron sus exigencias para animarles a pagar**, mientras que en el caso de las instituciones de educación superior, fue el **éxito de las negociaciones**. Esto puede haber sido uno de los motivos por los que las instituciones de educación superior declararon haber pagado los rescates más bajos en la encuesta de este año.

Por último, tanto la educación primaria y secundaria como la educación superior señalaron múltiples factores (tres y dos, respectivamente) que explican que pagaran menos por el rescate, lo que subraya aún más la situación compleja y polifacética que viven las víctimas del ransomware.

El impacto del ransomware en el negocio

Costes de recuperación en el sector educativo

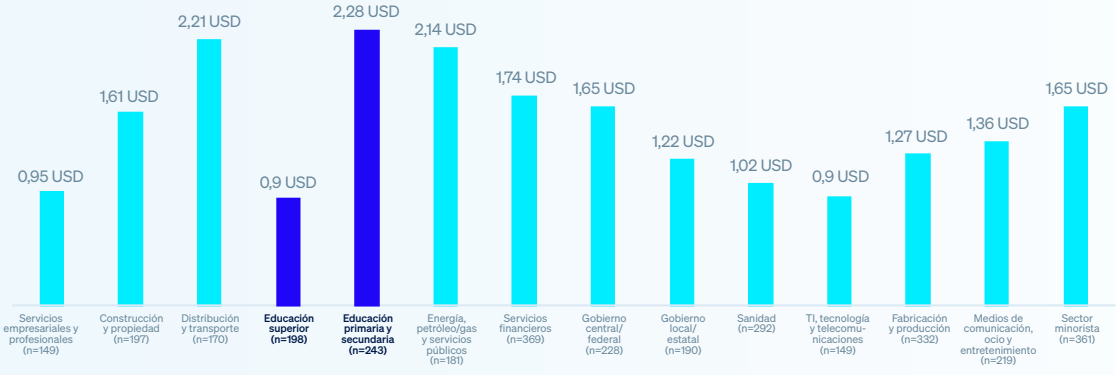
En 2025, los costes medios de recuperación (sin contar el pago de rescates) para las instituciones educativas se redujeron drásticamente. La educación superior registró una caída del 77 % hasta los 0,90 millones USD (el coste de recuperación más bajo de todos los sectores encuestados). En marcado contraste, a pesar de una reducción del 39 % con respecto a los 3,76 millones USD registrados en 2024, las organizaciones de educación primaria y secundaria acusaron el coste medio de recuperación más alto de todos los sectores analizados: 2,28 millones USD. Esto posiblemente se deba a los limitados recursos de TI y a los sistemas obsoletos y fragmentados típicos del sector.

	2023	2024	2025
Educación primaria y secundaria	1,59 MUSD (n=159)	3,76 MUSD (n=197)	2,28 MUSD (n=243)
Educación superior	1,06 MUSD (n=157)	4,02 MUSD (n=190)	0,90 MUSD (n=198)

¿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.)? Números base en la tabla.

Al analizar el desglose por sector, los costes de recuperación varían notablemente. Por detrás de la educación superior, las organizaciones de distribución y transporte registraron el coste medio más elevado para rectificar incidentes, situado en 2,21 millones USD. Por su parte, el sector de TI, tecnología y telecomunicaciones registró el coste más bajo, junto con la educación superior: 0,90 millones USD.

Gráfico 12: oste de recuperación del ransomware por sector (en millones USD)



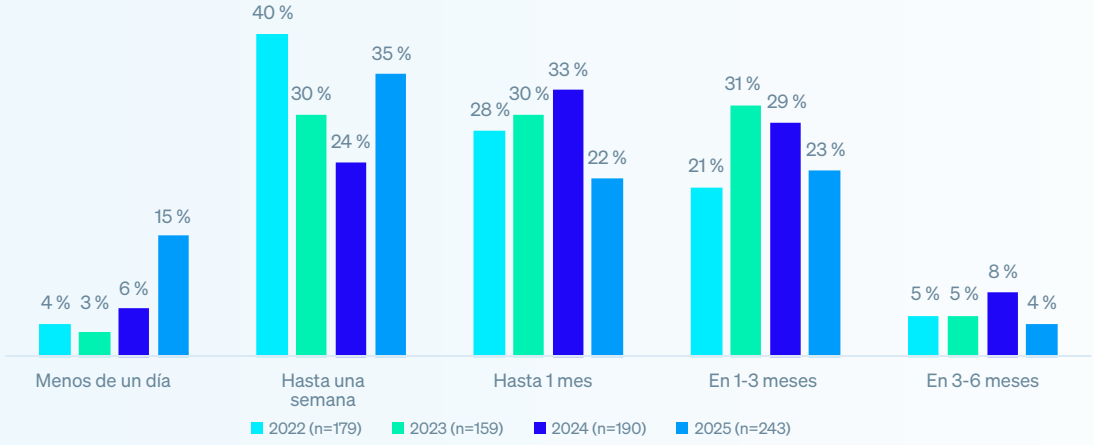
¿Cuál fue el coste aproximado que tuvo que asumir su organización para rectificar los perjuicios del ataque de ransomware más significativo (teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de dispositivos, el coste de redes, las oportunidades perdidas, etc.)? Los números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

Tiempo de recuperación en el sector educativo

Los datos revelan que, en 2025, **las instituciones educativas se recuperan más rápidamente de los ataques de ransomware.** La mitad de las instituciones de educación primaria y secundaria y el 59 % de las de educación superior se recuperaron completamente en una semana (ambas cifras representan un aumento considerable con respecto al 30 % registrado en 2024). Por otra parte, la proporción de las que tardaron entre uno y tres meses en recuperarse se redujo al 23 % en el caso de la educación primaria y secundaria y al 14 % en el de la educación superior, frente al 29 % y el 34 %, respectivamente.

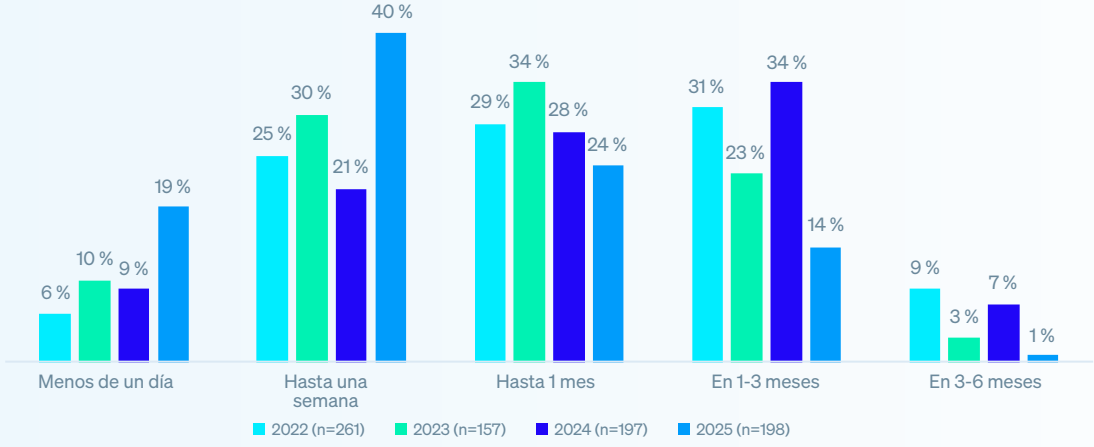
En general, el 95 % de las víctimas del sector educativo se recuperaron completamente en menos de tres meses, lo que pone de relieve la creciente resiliencia y capacidad de recuperación de todo el sector.

Gráfico 13: tiempo de recuperación de las instituciones de educación primaria y secundaria tras ataques de ransomware 2022 - 2025



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

Gráfico 14: tiempo de recuperación de las instituciones de educación superior tras ataques de ransomware 2022 - 2025



Como era de esperar, las organizaciones educativas cuyos datos se habían cifrado tardaron más en recuperarse que aquellas que pudieron detener el cifrado: el 13 % de las que se habían visto afectadas por el cifrado se recuperaron por completo en un día, frente al 19 % de aquellas cuyos adversarios no lograron cifrar los datos.

El impacto del ransomware a nivel humano

La encuesta evidencia que sufrir el cifrado de datos en un ataque de ransomware tiene repercusiones significativas para los equipos de TI/ciberseguridad del sector educativo, ya que todos los encuestados afirman que sus equipos se han visto afectados de alguna manera.

Gráfico 15: las consecuencias del cifrado de datos para los equipos de TI/ciberseguridad

Educación primaria y secundaria		Educación superior	
41 %	Aumento de la **presión** por parte de los cargos directivos	53 %	Aumento de la **presión** por parte de los cargos directivos
40 %	Aumento continuo de la **carga de trabajo**	50 %	Cambios en la estructura del **equipo o la organización**
37 %	Aumento de **la ansiedad o el estrés** por futuros ataques	40 %	Aumento de **la ansiedad o el estrés** por futuros ataques
37 %	Sentimiento de **culpa** por no haber podido detener el ataque	37 %	Aumento continuo de la **carga de trabajo**
36 %	Mayor **reconocimiento** por parte de los cargos directivos	36 %	Sentimiento de **culpa** por no haber podido detener el ataque
34 %	Cambio en **las prioridades o el enfoque del equipo**	34 %	Mayor **reconocimiento** por parte de los cargos directivos
29 %	Cambios en la estructura del **equipo o la organización**	33 %	Se ha sustituido a los **responsables** del equipo
26 %	Bajas del personal por problemas de **estrés o salud mental**	31 %	Cambios en la estructura del **equipo o la organización**
26 %	Se ha sustituido a los **responsables** del equipo	31 %	Bajas del personal por problemas de **estrés o salud mental**

¿Qué repercusiones ha tenido el ataque de ransomware en las personas de su equipo de TI/ciberseguridad, si las hay? n=70 (educación primaria y secundaria), 115 (educación superior)

Recomendaciones

Aunque las organizaciones educativas han percibido varios cambios con respecto al ransomware durante el último año, este sigue siendo una importante amenaza. 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 del ransomware y otras amenazas. Las conclusiones de este informe pueden ayudarle a reforzar sus defensas, perfeccionar su respuesta a las amenazas y limitar el impacto del ransomware en su empresa y en su personal. Céntrese en estas cuatro áreas clave para adelantarse a los ataques:

- **Prevención**. La defensa más eficaz contra el ransomware es aquella en la que el ataque nunca se produce, porque los adversarios no han podido infiltrarse en su organización. Tome medidas para eliminar las causas raíz técnicas y organizativas que se resaltan en este informe.
- **Protección**. Es imprescindible contar con una base sólida de seguridad. 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.
- **Detección y respuesta.** Cuanto antes detenga un ataque, mejores serán sus resultados. Ahora, la detección y respuesta a las amenazas 24/7 es una capa esencial de defensa. Si no dispone de los recursos o las capacidades para llevarla a cabo internamente, recurra a un proveedor de detección y respuesta gestionadas (MDR) de confianza.
- **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. Asegúrese de hacer copias de seguridad de calidad y practique con regularidad la restauración de datos a partir de ellas para agilizar la recuperación en caso de sufrir un ataque.

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

Obtenga más información sobre el ransomware y cómo Sophos puede ayudarle a proteger su organización.

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

© Copyright 2025. Sophos Ltd. Todos los derechos reservados.
Constituida en Inglaterra y Gales N.º 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido
Sophos es la marca registrada de Sophos Ltd. Todos los demás productos y empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.

2025-08-28 WP (NP)

SOPHOS