INFORME

El estado del ransomware en el sector educativo 2026

Resultados de una encuesta independiente realizada a 226 responsables de TI y ciberseguridad del sector educativo en 17 países cuyas organizaciones se vieron afectadas por el ransomware en el último año.

SOPHOS

Introducción

Le damos la bienvenida a la sexta edición del informe anual Sophos: El estado del ransomware en la educación, que revela la realidad del ransomware tanto para los proveedores de educación primaria y secundaria (incluyendo K-12, escuelas primarias y secundarias, normalmente para estudiantes menores de 18 años) como para los de educación superior (universidades, colegios e instituciones equivalentes, normalmente para estudiantes mayores de 18 años) en 2026.

El informe de este año también arroja nueva luz sobre áreas previamente inexploradas, como dónde comienzan los ataques en el entorno, el papel defensivo de la autenticación multifactor (MFA) y los firewalls, y la conexión entre los ataques de identidad y el ransomware.

En el informe, que se basa en las experiencias reales de 226 responsables de TI y ciberseguridad (131 de instituciones de educación primaria y secundaria y 95 de educación superior afectadas por el ransomware durante el último año), se ofrecen datos clave sobre:

- Métodos de ataque y defensa
- El cifrado y la recuperación de datos
- El importe del rescate exigido y el importe abonado
- El impacto a nivel empresarial y humano

Nota: A lo largo de este informe, el término «encuesta general» se refiere a los resultados de los encuestados de todos los sectores analizados. Los 226 encuestados del sector educativo forman parte de un grupo más amplio de 2158 encuestados de 15 sectores industriales.

Acerca de la encuesta

Este informe se basa en los resultados de una encuesta independiente y desvinculada del proveedor encargada por Sophos. La encuesta se centró en la experiencia de las organizaciones ante los ataques de ransomware y las intrusiones basadas en la identidad, realizando un seguimiento año tras año de los índices de pago del rescate, los costes de restauración, los plazos de recuperación y muchos otros indicadores. Las respuestas se recabaron entre enero y marzo de 2026 y se basan en las experiencias de los encuestados durante los 12 meses anteriores.

Los participantes procedían de 17 países y de 15 sectores económicos, de una amplia variedad de sectores, tanto del ámbito público como del privado, y la distribución de tamaños de empresa (con un número de empleados comprendido entre 100 y 5.000) se ha mantenido proporcionalmente constante a lo largo de los seis años de historia de la encuesta. Todos los puntos de datos financieros son en dólares estadounidenses (USD).

Principales conclusiones

- **Los ataques de identidad, especialmente los basados en correo electrónico, fueron elevados en los sectores educativos.**
  - El 77 % de las víctimas de la educación superior y el 71 % de la educación primaria y secundaria confirmaron que su ataque de ransomware también fue su ataque de identidad más significativo, ambos por encima del índice general de la encuesta del 67 % (todos los sectores).
  - El correo electrónico malicioso fue la principal causa raíz técnica de los ataques de ransomware en la educación primaria y secundaria (31 %) y la educación superior (29 %).
  - Los enfoques basados en la identidad (por ejemplo, correo electrónico malicioso, phishing, compromiso de credenciales o fuerza bruta) iniciaron el 85 % de los ataques en toda la educación, por encima del índice del 79 % en todos los sectores.
- **Las deficiencias operativas en el sector educativo fueron superiores a las de la encuesta general (todos los sectores).**
  - La carencia más notable de la educación superior era la falta de conocimientos especializados: El 53 % afirmó que carecía de las habilidades para detectar y detener el ataque a tiempo, frente al 35 % de la encuesta general.
  - Las principales causas raíz operativas en la educación primaria y secundaria fueron los errores humanos (52 %), la falta de protección (47 %), las lagunas de seguridad desconocidas (42 %) y la falta de personal o capacidad (41 %).
- **El cifrado resultante de los ataques de ransomware aumentó drásticamente en la educación primaria y secundaria.**
  - El índice de cifrado de datos de la educación primaria y secundaria se duplicó con creces, pasando del 29 % en 2025 al 61 % en 2026.
  - El 58 % de los ataques del sector educativo comportaron el cifrado de datos, cerca del 56 % del índice general de la encuesta.
- **Las instituciones educativas dependían en gran medida de las copias de seguridad para restaurar los datos.**
  - El 77 % de las instituciones de educación primaria y secundaria restauraron datos cifrados mediante copia de seguridad, por encima del índice general de la encuesta del 66 %.
  - El 69 % de las instituciones de educación superior también se recuperaron gracias a las copias de seguridad.
- **Los centros educativos pagaron menos que la media general, pero registraron un mayor número de pagos de rescate superiores a 5 millones USD.**
  - La mediana de la cantidad exigida en concepto de rescate en el sector educativo fue superior a la de la encuesta general, con 775 200 USD (frente a los 698 000 USD), mientras que la mediana del pago de rescate fue inferior: 515 000 USD (frente a los 769 000 USD de la encuesta general).
  - La mediana de las peticiones de rescate en el sector ha bajado dos años consecutivos, mientras que los pagos aumentaron en 15 000 USD entre el informe de 2025 y el de 2026.
  - Las instituciones educativas tenían más probabilidades de pagar 5 millones de dólares o más (23 % frente al 16 % de la encuesta general).
- **En el ámbito educativo, la recuperación costó más y llevó más tiempo.**
  - Los costes medios de recuperación en el ámbito educativo alcanzaron los 2,26 millones USD, por encima de la cifra global de la encuesta, que fue de 1,7 millones USD.
  - Los costes de recuperación en el sector educativo han subido desde el informe de 2025, pasando de 1,66 millones a 2,26 millones USD, y los costes de la educación superior han aumentado en más de 1 millón USD.
  - El 26 % de las instituciones educativas necesitaron de uno a tres meses para recuperarse por completo de un ataque de ransomware, aproximadamente el doble del índice del 14 % en todos los sectores.
  - La educación primaria y secundaria fue la que registró el mayor porcentaje de recuperaciones a largo plazo: El 31 % tardó un mes o más en recuperarse, más que cualquier otro sector.
- **El coste humano para los equipos de seguridad se intensificó.**
  - El 53 % de los equipos de educación superior registraron un aumento de la presión por parte de los directivos, frente al 40 % en todos los sectores.
  - Alrededor del 39 % de los equipos educativos afirmaron ausencias del personal debido a problemas de estrés o salud mental, frente al 29 % en todos los sectores.

Métodos de ataque y defensa

Causas raíz de los ataques

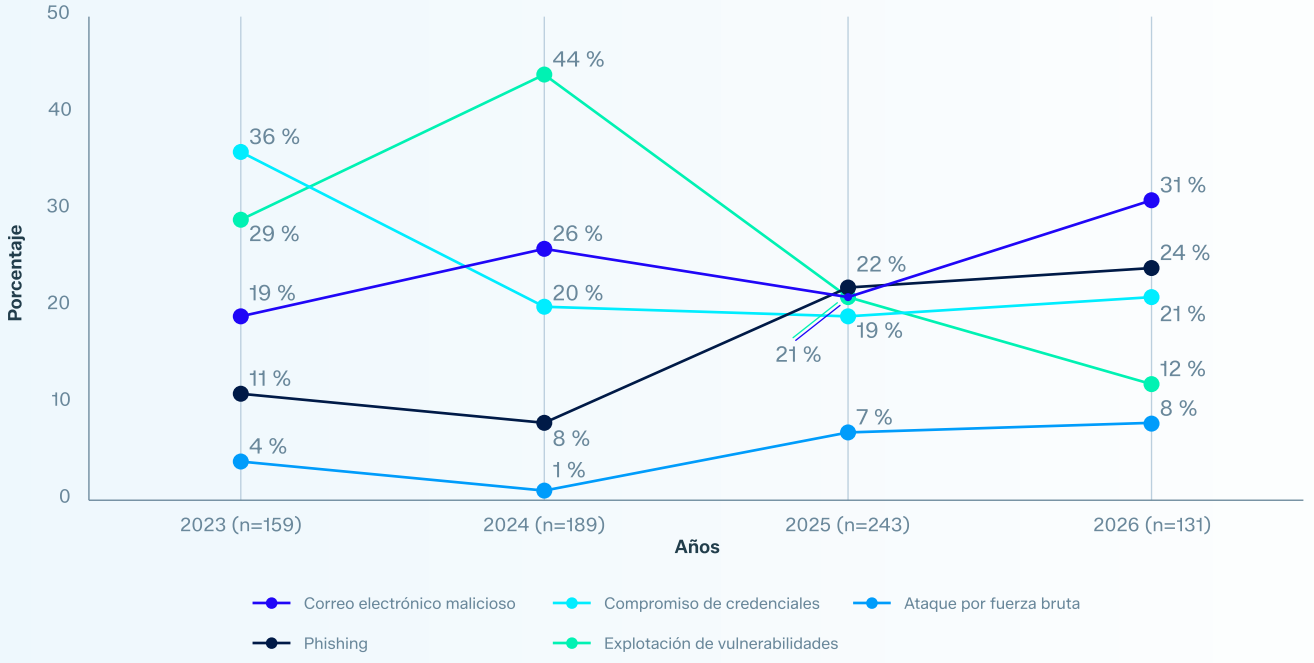
Los datos educativos de este año reflejan el mismo cambio observado en todos los sectores: los ataques basados en la identidad están creciendo.

El correo electrónico malicioso fue la causa raíz técnica más frecuente en la educación primaria y secundaria (31 %), seguido del phishing (24 %) y del compromiso de credenciales (21 %). La explotación de vulnerabilidades descendió al 12 %, lo que refleja la caída general observada en la encuesta que abarca todos los sectores hasta el 18 %.

85%

El porcentaje de ataques a instituciones educativas que comenzaron con un enfoque basado en la identidad (por ejemplo, correo electrónico malicioso, phishing, compromiso de credenciales o fuerza bruta), por encima del índice general de la encuesta del 79 %.

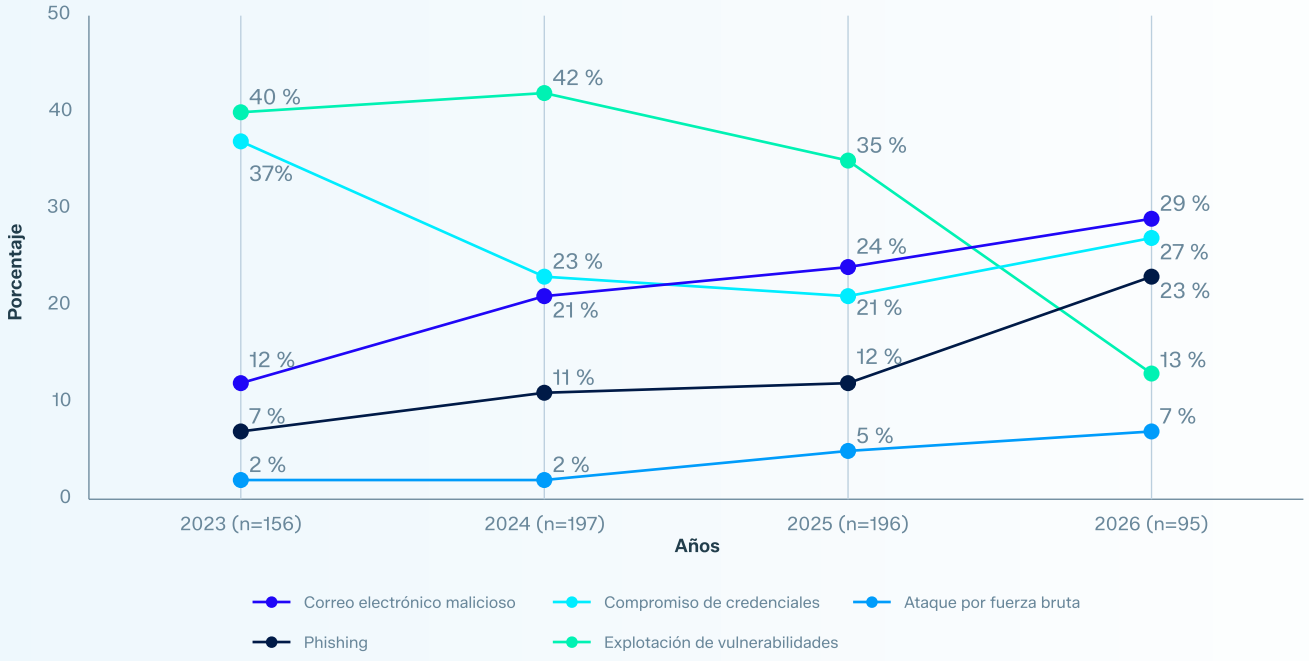
Causa raíz técnica de los ataques de ransomware 2023–2026: Educación primaria y secundaria



¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año?
Las descargas y las respuestas «No lo sé» se han excluido de la tabla para mayor claridad visual.
Es posible que el total de los porcentajes no sume el 100 %. Números base en la tabla.

Las instituciones de educación superior también registraron un descenso en la explotación de vulnerabilidades. Ese vector cayó al 13 % en el informe de 2026, frente al 35 % de 2025. **El correo electrónico malicioso (29 %) y el compromiso de credenciales (27 %) son, prácticamente, las principales causas,** seguidas muy de cerca por el phishing, con un 23 %. Tanto el sector de la educación primaria y secundaria como el de la educación superior señalan los ataques basados en el correo electrónico como las principales causas, lo que es coherente con la encuesta general, en la que el correo electrónico malicioso (26 %) y el phishing (24 %) representan juntos la mitad de todos los incidentes.

Causa raíz técnica de los ataques de ransomware 2023–2026: Educación superior

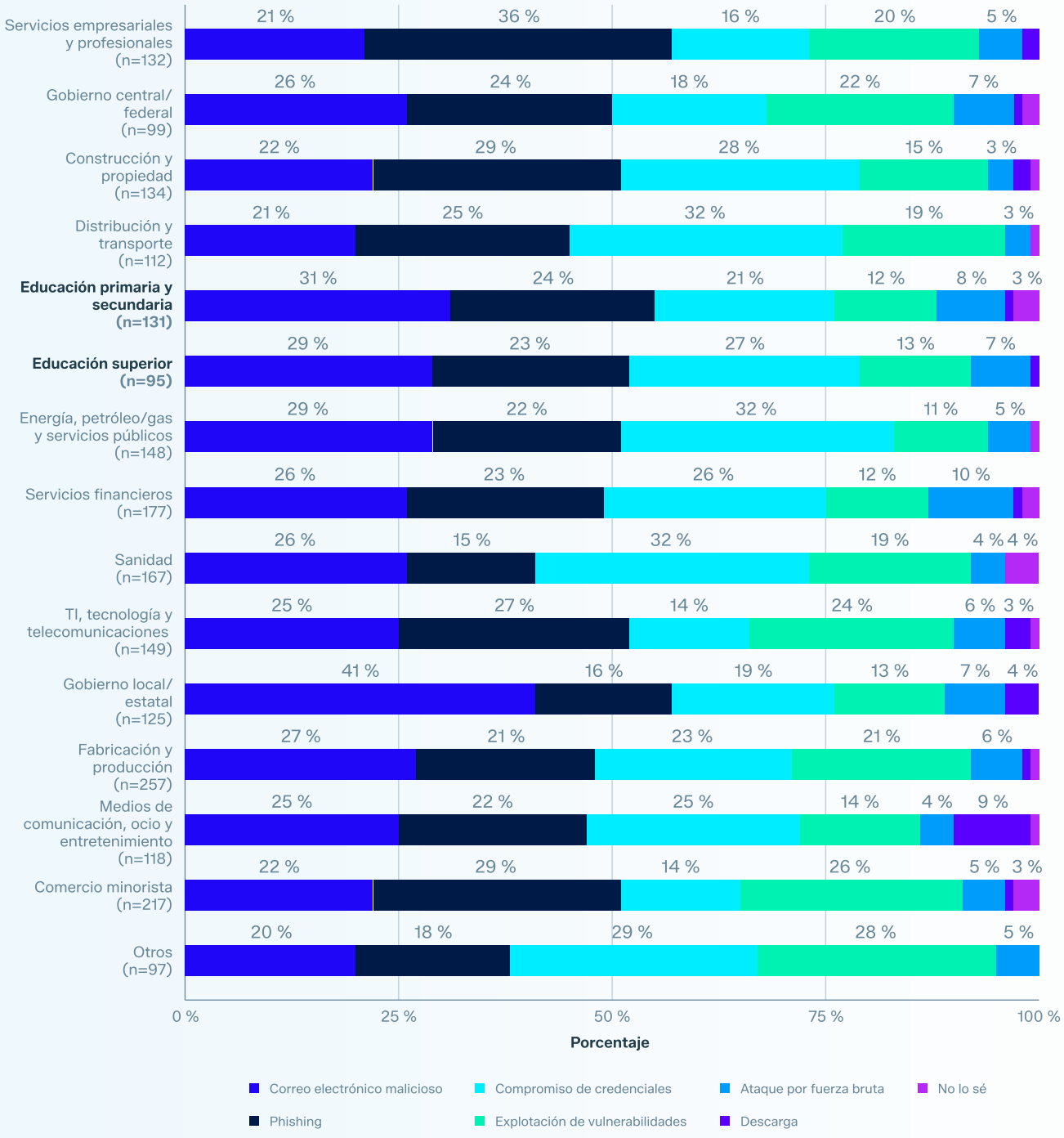


¿Conoce la causa raíz del ataque de ransomware que su organización sufrió en el último año?
Las descargas y las respuestas «No lo sé» se han excluido de la tabla para mayor claridad visual.
Es posible que el total de los porcentajes no sume el 100 %. Números base en la tabla.

En conjunto, los vectores basados en **la identidad (por ejemplo, correo electrónico malicioso, phishing, compromiso de credenciales y ataques por fuerza bruta) representaron el 85 % de los ataques contra instituciones educativas, por encima del 79 % del índice de la encuesta general**. La educación superior registró el porcentaje más alto, con un 86 %, seguida de la educación primaria y secundaria, con un 84 %. En otras palabras, aproximadamente seis de cada siete ataques contra el sector educativo comenzaron con un enfoque basado en la identidad, lo que refuerza por qué la seguridad de la identidad es fundamental para las defensas del sector.

La educación refleja el cambio más amplio de todos los sectores hacia más ataques basados en correos electrónicos y menos informes de explotación de vulnerabilidades. Sin embargo, los expertos de Sophos prevén que los exploits vuelvan a aumentar, ya que a las empresas les cuesta mantenerse al día con los parches para las vulnerabilidades detectadas por la IA de frontera.

Causa raíz técnica por sector (2026)



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

Factores de vulnerabilidad de las organizaciones

Las instituciones educativas mencionaron una amplia variedad de problemas relacionados con la protección, la dotación de recursos y las deficiencias en materia de seguridad. De las tres categorías consolidadas, el 63 % de las instituciones educativas mencionaron problemas de recursos (falta de personal o de conocimientos), seguidos de problemas de protección (62 %) y lagunas de seguridad (62 %).

¿Por qué cree que su organización sufrió un ataque de ransomware? n=226. Respuestas consolidadas.

El conjunto del sector educativo ha registrado un índice más alto que el de la encuesta general en casi todas las causas raíz operativas, siendo las lagunas de seguridad conocidas la única excepción. Si separamos la educación primaria y secundaria de la educación superior, se ponen de manifiesto dos puntos débiles distintos.

La principal debilidad de la educación superior fue la falta de conocimientos especializados. El 53 % afirmó que carecía de las habilidades o los conocimientos necesarios para detectar y detener el ataque a tiempo, frente al 35 % de la encuesta general, una brecha de 18 puntos porcentuales y la mayor.

Las debilidades de la educación primaria y secundaria se centran en la capacidad y las herramientas. Según el 52 % de los centros de educación primaria y secundaria (frente al 35 % en el conjunto de todos los sectores), el error humano fue el principal problema; el 47 % mencionó la falta de protección, y el 41 %, la falta de personal o de capacidad.

53 %

El porcentaje de víctimas de la educación superior que afirmaron carecer de las habilidades o los conocimientos necesarios para detectar y detener el ataque a tiempo, 18 puntos por encima de la encuesta general y su mayor punto débil.

Causas raíz operativas: Educación primaria y secundaria frente a todos los sectores

Causa raíz operativa	Educación primaria y secundaria (n=131)	Educación superior (n=95)	Todos los sectores (n=2158)
Falta de protección	47 %	36 %	36 %
Laguna de seguridad desconocida	42 %	38 %	36 %
Laguna de seguridad conocida	33 %	35 %	36 %
Falta de personal/capacidad	41 %	37%	35 %
Error humano	52 %	36 %	35 %
Falta de conocimientos especializados	33 %	53 %	35 %
Protección deficiente	38 %	39 %	33 %

¿Por qué cree que su organización sufrió un ataque de ransomware? Se permiten múltiples respuestas. Números base en la tabla.

En comparación con otros sectores, la educación tuvo dificultades debido a la falta de protección y de conocimientos especializados. La tabla siguiente muestra los sectores colocados en la columna de la causa raíz operativa que más citaron.

Principales causas raíz operativas de los ataques de ransomware por sector

¿Por qué cree que su organización sufrió un ataque de ransomware? Se permiten múltiples respuestas. Los sectores que se relacionan con varias causas están marcados con un asterisco (*). n = 2158.

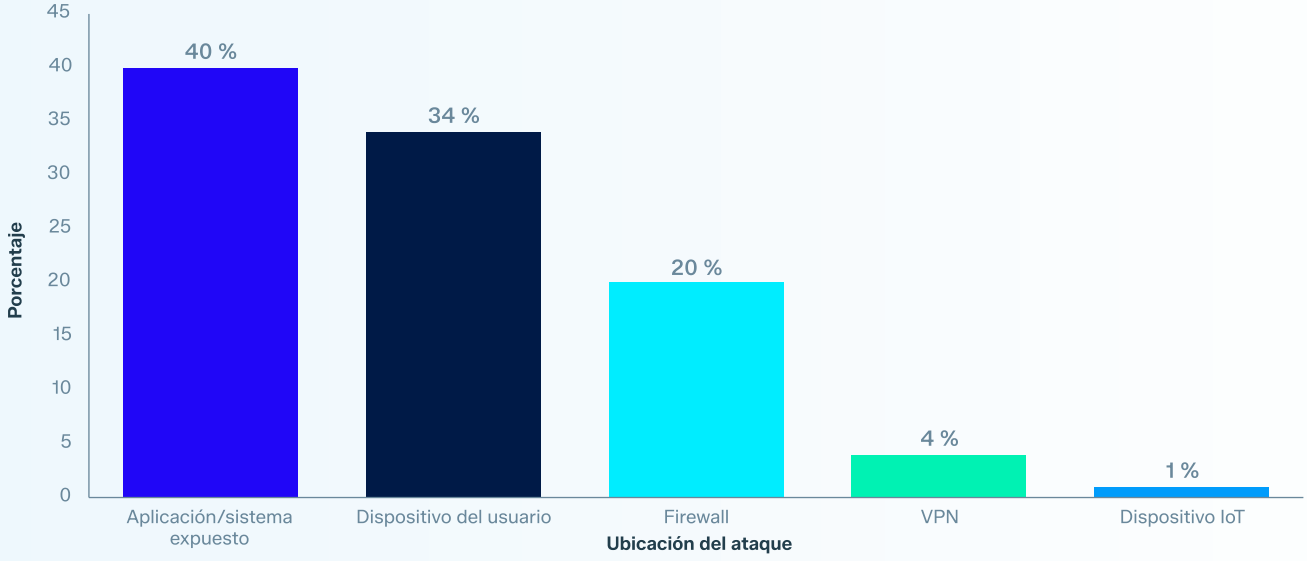
NUEVA INVESTIGACIÓN

Dónde se originan los ataques

Una nueva investigación de este año añade una pregunta sobre dónde comenzaron los ataques en el entorno, específicamente entre los incidentes que comenzaron con la explotación de una vulnerabilidad, el compromiso de credenciales o un ataque por fuerza bruta.

En el ámbito educativo, las aplicaciones y sistemas expuestos fueron el punto de entrada más común (40 %), seguidos de los dispositivos de usuario (34 %) y de los firewalls (20 %). Estas cifras siguen de cerca la encuesta general (38 %, 30 % y 21 % respectivamente), de modo que la educación no muestra ninguna divergencia significativa en este sentido.

Dónde se originan los ataques de ransomware: Conjunto del sector educativo



Ha indicado que la causa raíz fue la explotación de una vulnerabilidad, el compromiso de credenciales o un ataque por fuerza bruta. ¿Dónde ocurrió esto en tu entorno? Combina educación superior y educación primaria y secundaria. n=99

NUEVA INVESTIGACIÓN

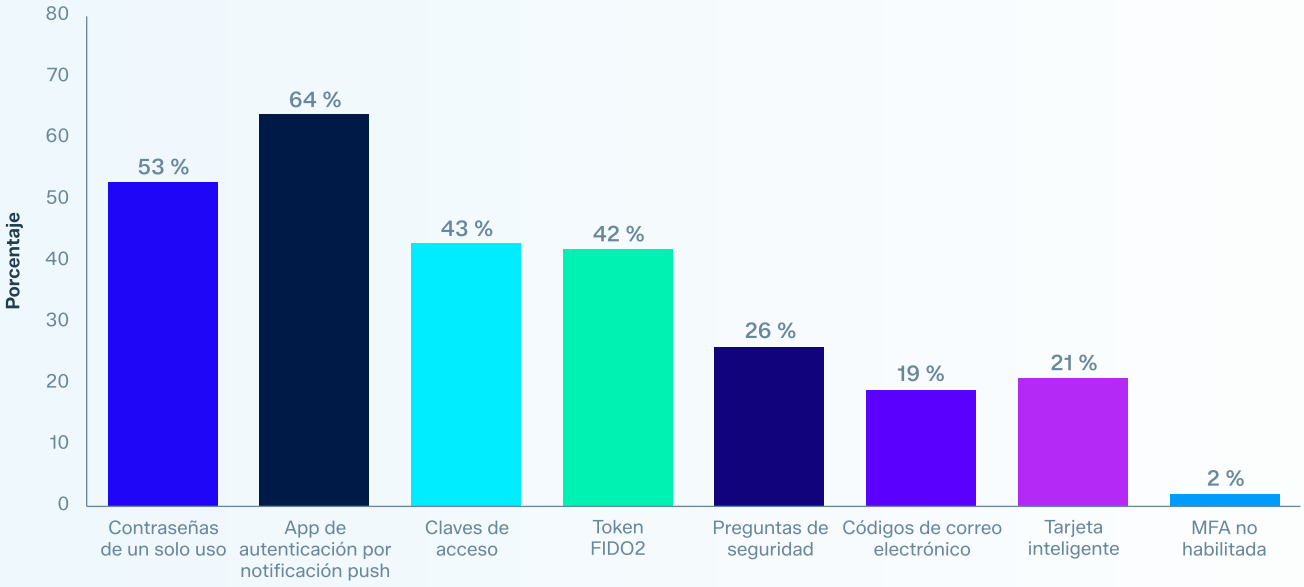
El papel de la autenticación multifactor (MFA)

También analizamos los métodos de MFA que se utilizaban en el momento del ataque entre las instituciones educativas cuyos ataques tuvieron su origen en el compromiso de credenciales. Casi todas las víctimas del sector educativo tenían habilitada algún tipo de MFA (98 %), lo que coincide con el resultado de la encuesta general (97 %), según el cual la MFA estaba implementada en la mayoría de los ataques basados en credenciales.

Sin embargo, entre las instituciones educativas a las que se les preguntó sobre la MFA, el 81 % sufrió el cifrado de sus datos a pesar de tener la MFA activada. Esto sugiere que la autenticación multifactor no se desplegó de forma exhaustiva en todos los sistemas críticos, que los atacantes encontraron formas de eludir las protecciones de la autenticación multifactor o que los vectores de ataque no dependían únicamente del compromiso de credenciales.

Las aplicaciones basadas en notificaciones push (64 %) y las contraseñas de un solo uso (53 %) fueron los métodos de autenticación más utilizados en el ámbito educativo.

Métodos de autenticación multifactor habilitados en el momento del ataque: Conjunto del sector educativo



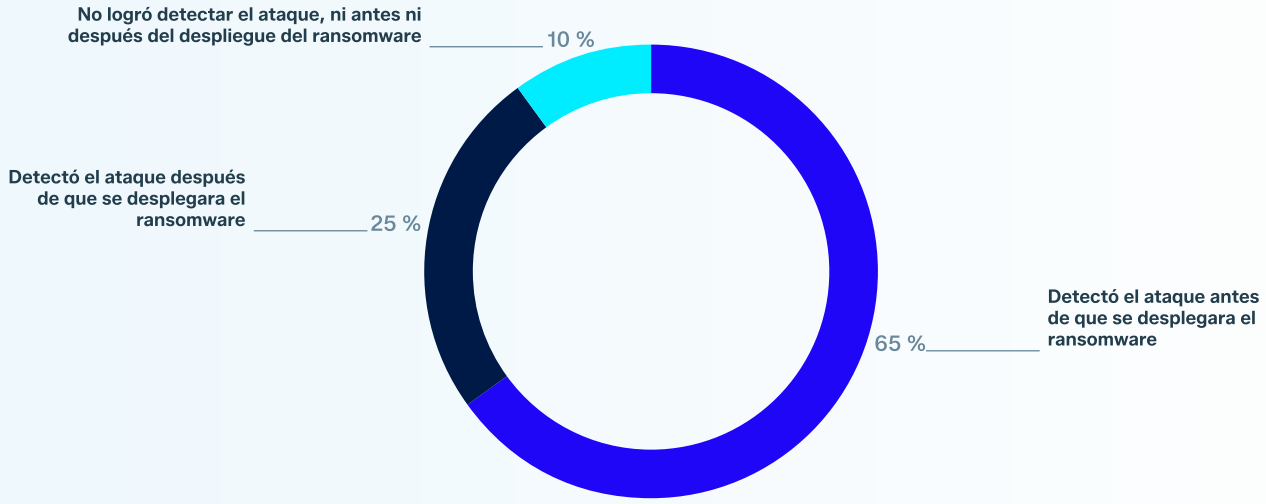
¿Qué tipo de autenticación multifactor estaba habilitada en el momento del ataque, de ser el caso? Se permiten múltiples respuestas.
Base: El ataque se produjo debido al compromiso de credenciales. Combina educación superior y educación primaria y secundaria. n=53.

NUEVA INVESTIGACIÓN

El papel de los firewalls

En el ámbito educativo, los firewalls identificaron la mayoría de los ataques, pero no siempre ayudaron a detenerlos. El 65 % de los proveedores afirmaron que su firewall identificó el ataque antes de que se desplegara el ransomware, el 25 % afirmaron que lo identificaron después y el 10 % afirmaron que no lo identificaron en absoluto. Esto refleja la encuesta general (61 %, 32 % y 7 %), con un ligero desplazamiento hacia los dos extremos del espectro.

¿Qué papel desempeñó el firewall a la hora de detectar el ataque?



¿Qué papel desempeñó el firewall a la hora de detectar el ataque? Combina educación superior y educación primaria y secundaria. n=226.

Entre esos casos de detección anticipada, las víctimas del sector educativo seguían teniendo sus datos cifrados el 51 % de las veces.

Los firewalls están haciendo un buen trabajo a la hora de recopilar datos para identificar ataques, pero los ataques siguen sin detenerse al mismo ritmo que se identifican. Los firewalls suelen registrar los datos necesarios para detectar y detener un ataque, pero es posible que no se conecten lo suficientemente profundamente con otros sistemas para reconocer la amenaza y responder a tiempo.

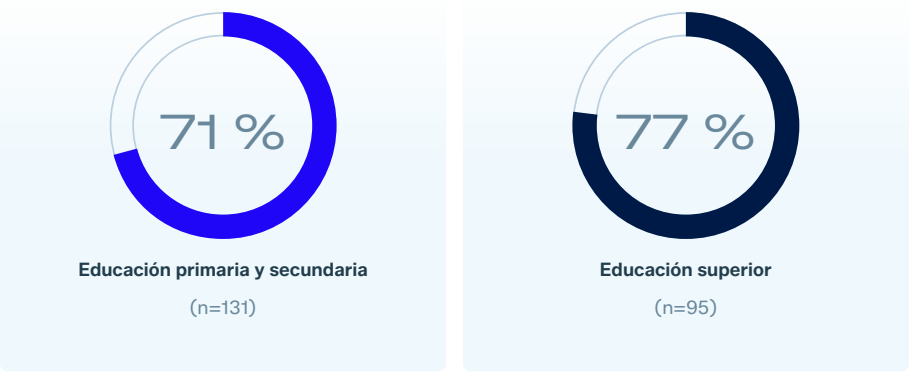
NUEVA INVESTIGACIÓN

La relación entre los ataques a la identidad y el ransomware

Uno de los resultados más claros de la encuesta es el vínculo directo entre los ataques de identidad y el ransomware. De todos los sectores, dos tercios de las víctimas de ransomware (67 %) confirmaron que el incidente coincidió con su ataque más significativo relacionado con la identidad. Sin embargo, el sector educativo supera esa cifra: un 71 % en la educación primaria y secundaria y un 77 % en la educación superior (un 73 % en conjunto).

Aunque no todos los ataques dieron lugar al cifrado de datos, el hallazgo muestra una fuerte superposición entre los ataques de identidad y el ransomware en el sector educativo.

El ataque de ransomware también fue su ataque más importante relacionado con la identidad



¿Su organización sufrió un ataque de ransomware que también fue un ataque de identidad? Organizaciones afectadas por el ransomware. Números base en los gráficos.

73 %

El porcentaje de víctimas del sector educativo cuyo incidente de ransomware fue el mismo evento que su ataque de identidad más significativo, por encima del índice general de encuesta del 67 %.

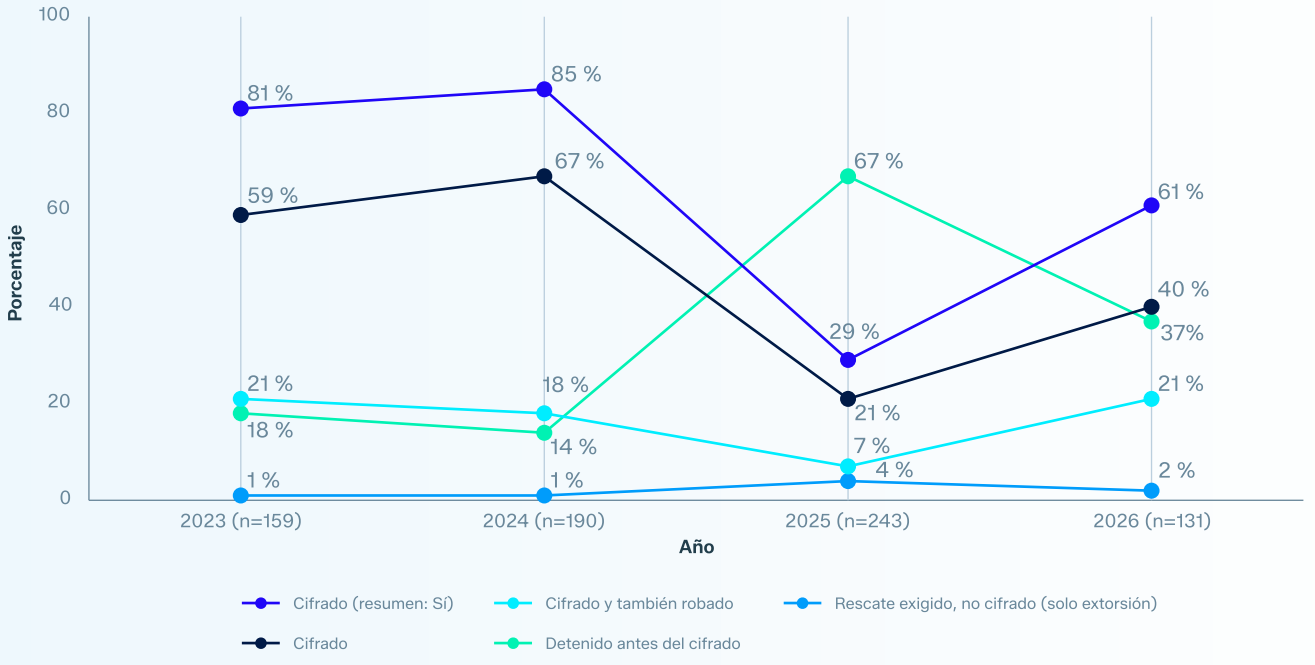
El cifrado y la recuperación de datos

Índice de cifrado de datos

Los resultados del informe El estado del ransomware en el sector educativo 2025 mostraron resultados muy positivos para la educación primaria y secundaria. Desafortunadamente, el informe de este año muestra que la educación primaria y secundaria retrocede más cerca de su tendencia anterior.

Después de que el índice de cifrado de la educación primaria y secundaria descendiera al 29 % en el informe de 2025, el más bajo de todos los sectores de ese año, **el porcentaje de ataques contra la educación primaria y secundaria que lograron cifrar los datos se duplicó con creces hasta el 61 % en 2026** (por encima del índice general de encuesta del 56 %). Este año, solo el 37 % de los ataques se detuvieron antes del cifrado por parte de la educación primaria y secundaria, lo que supone un descenso respecto al 67 % del informe del año pasado.

Índice de cifrado de datos a lo largo del tiempo: Educación primaria y secundaria

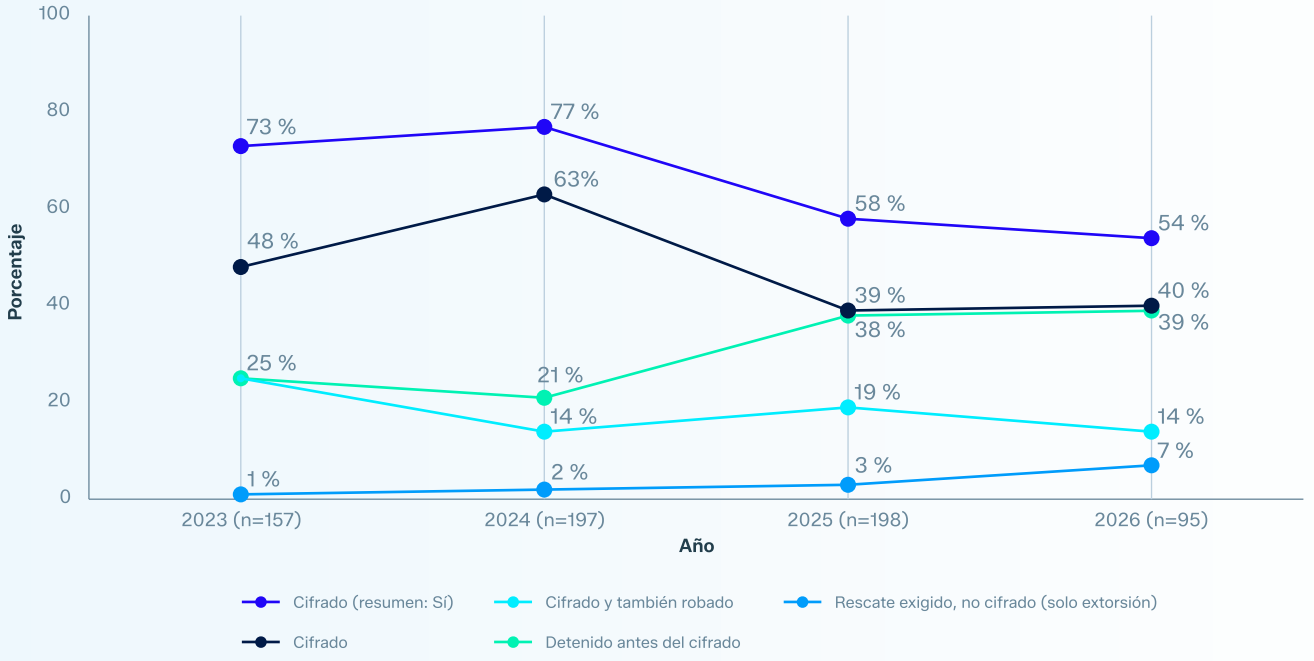


¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Números base en la tabla.
La línea "Cifrado (resumen: Sí)" de este gráfico es la suma de las respuestas "Cifrado" y "Cifrado y también robado".

La doble extorsión (donde los datos se cifran y también se roban) resurgió en la educación primaria y secundaria, pasando del 7 % en 2025 al 21 % en 2026, lo que está en línea con sus niveles anteriores a 2025. Estos ataques ofrecen a los atacantes un segundo punto de apalancamiento. Los ataques de solo extorsión **(en los que se pide un rescate sin cifrar los datos)** bajaron ligeramente, del 4 % al 2 %, en el ámbito de la educación primaria y secundaria.

La educación superior se mantuvo más estable. Su índice de cifrado disminuyó ligeramente hasta el 54 % en 2026, frente al 58 % en 2025, lo que le mantuvo cerca de la encuesta general.

Índice de cifrado de datos a lo largo del tiempo: Educación superior



¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware? Números base en la tabla. La línea "Cifrado (resumen: Sí)" de este gráfico es la suma de las respuestas "Cifrado" y "Cifrado y también robado".

En el caso de la educación superior, los ataques de solo extorsión aumentaron al 7 %, frente al 3 % de 2025, lo que vale la pena observar aunque sea un porcentaje pequeño.

El panorama para 2026 también vuelve a situar a la educación en su tendencia a largo plazo. En 2023 y 2024, el índice de cifrado de datos en la educación primaria y secundaria fue superior al de la educación superior; 2025 fue la excepción, cuando el índice de la educación primaria y secundaria se desplomó brevemente. El índice de cifrado de este año, del 61 % en la educación primaria y secundaria frente al 54 % en la educación superior, restablece la tendencia a largo plazo.encia a largo plazo.

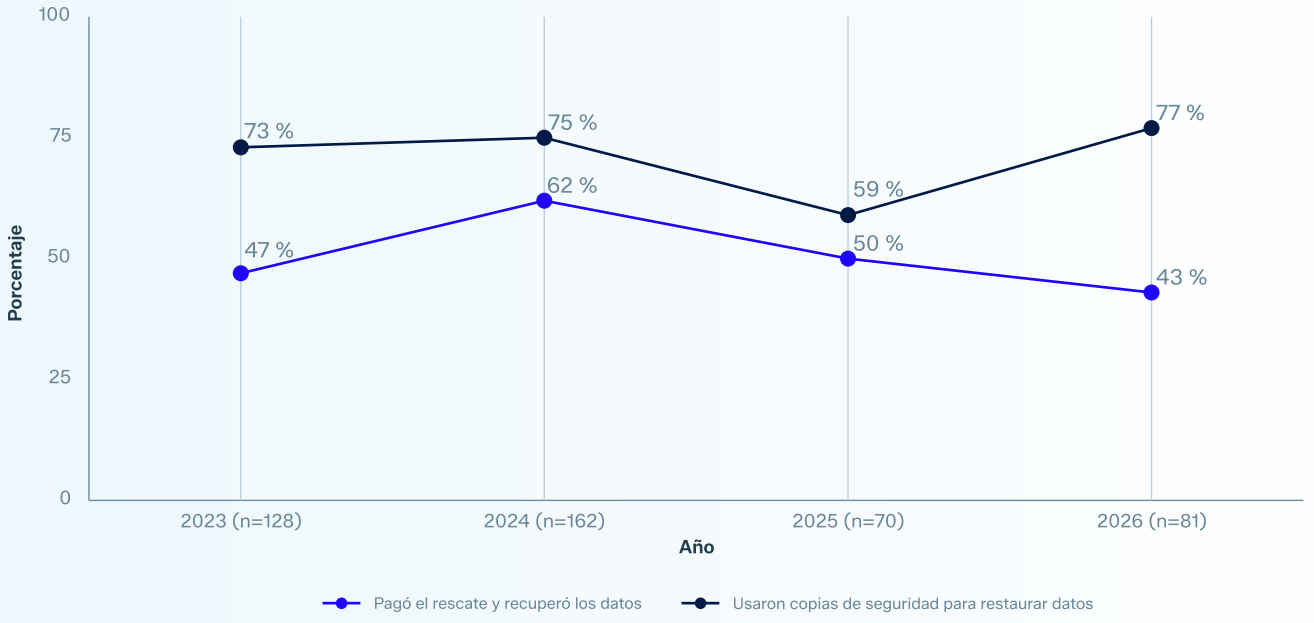
Cómo recuperaron las organizaciones los datos cifrados

Las copias de seguridad fueron el motor más importante de la recuperación en el sector educativo en 2026. Tras un descenso en 2025 (59 % en la educación primaria y secundaria, y 47 % en la educación superior), la recuperación basada en copias de seguridad se recuperó este año. **El 77 % de las instituciones de educación primaria y secundaria y el 69 % de las de educación superior restauraron datos a partir de copias de seguridad**, ambos por encima del índice general de encuesta del 66 %. El repunte sugiere que la educación ha renovado su inversión en infraestructura de copia de seguridad y está reconstruyendo la resiliencia frente a las peticiones de rescate.

77 %

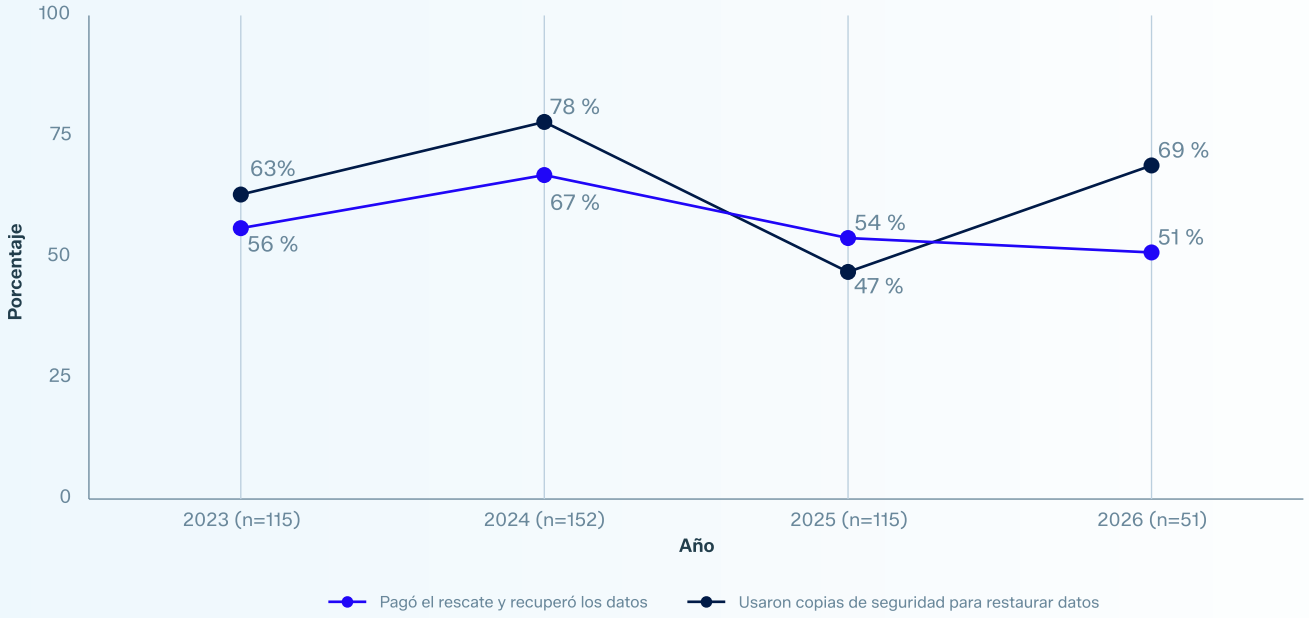
La proporción de instituciones de educación primaria y secundaria que restauraron datos cifrados a partir de copias de seguridad en 2026, por encima del índice general de encuesta del 66 %.

Métodos de recuperación de datos a lo largo del tiempo: Educación primaria y secundaria



¿Cómo recuperó su organización los datos? Se permiten múltiples respuestas. Números base en la tabla.

Métodos de recuperación de datos a lo largo del tiempo: Educación superior



¿Cómo recuperó su organización los datos? Se permiten múltiples respuestas. Números base en la tabla.

Por otro lado, el sector educativo paga cada vez menos rescates. **La proporción de proveedores que pagaron el rescate y recuperaron datos ha disminuido por dos años consecutivos**, del 62 % (2024) al 50 % (2025) al 43 % (2026) en la educación primaria y secundaria y del 67 % al 54 % al 51 %, respectivamente, en la educación superior.

Con el aumento de las restauraciones a partir de copias de seguridad y el descenso de recuperación a cambio de pago, el sector educativo se está recuperando más gracias a sus propias capacidades que a la cooperación de los atacantes.

Importe del rescate exigido e importe abonado

Peticiones de rescate

El sector educativo se enfrentó a peticiones de rescate más elevadas que otros sectores en la encuesta general. La mediana de la cantidad exigida a una institución educativa fue de 775 200 USD, por encima de la mediana de 698 000 USD para todos los sectores. La distribución también se inclinó hacia las cantidades más altas: **la mitad de las peticiones de rescate (50 %) eran de 1 millón USD o más**, y una cuarta parte (25 %) de 5 millones USD o más, en comparación con el 46 % y el 23 %, respectivamente, en la muestra de todos los sectores.

Nota: Se han eliminado de estos datos los rescates atípicos de 40 millones USD o más.

Petición de rescate (mediana)

	2025	2026
Educación	0,98 MUSD (n=185)	0,78 MUSD (n=132)
Todos los sectores	1,32 MUSD (n=1700)	0,70 MUSD (n=1214)

¿A cuánto ascendía el rescate exigido por los atacantes? Base: organizaciones cuyos datos fueron cifrados. Números base en la tabla.

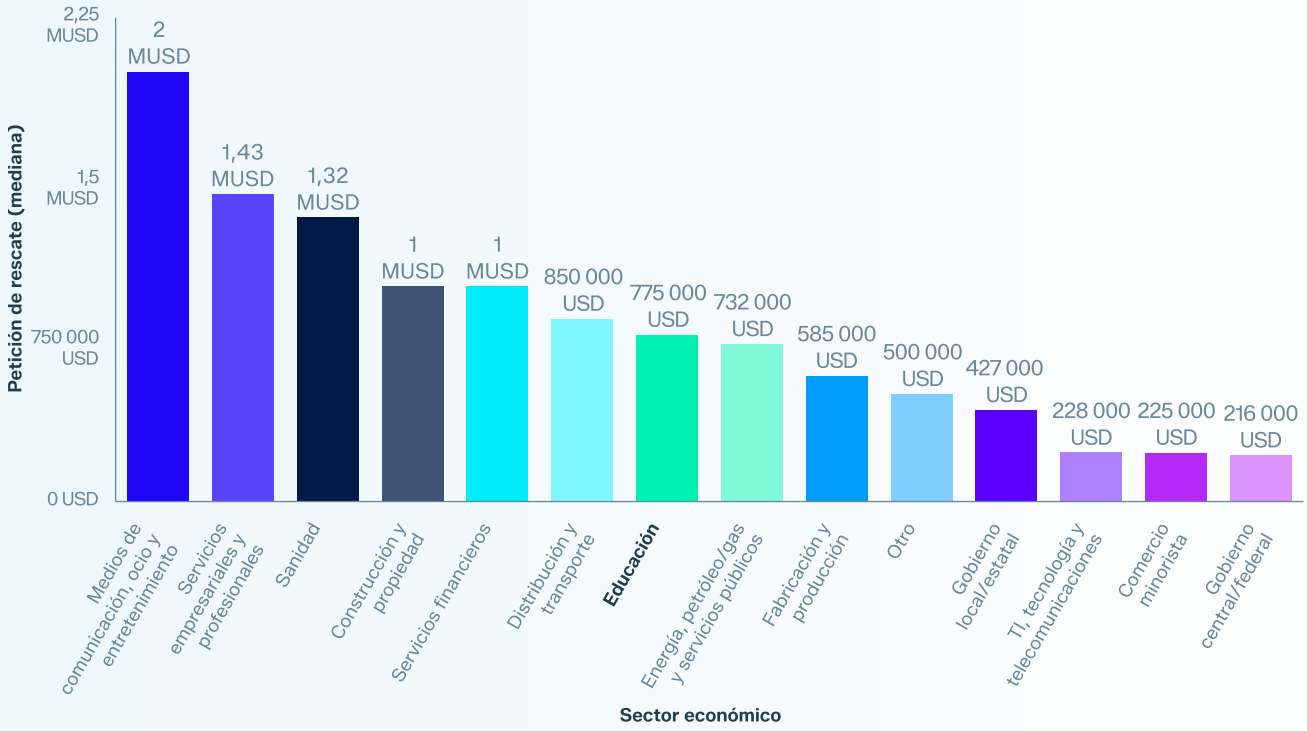
En comparación con otros sectores, la educación se sitúa en una posición intermedia. La mediana de las peticiones de rescate del sector es inferior a la de los sectores con las peticiones más altas, como los medios de comunicación, el ocio y el entretenimiento (2 millones USD) y los servicios empresariales y profesionales (1,43 millones USD), pero muy por encima de la de los sectores con las peticiones más bajas, como el gobierno central (216 500 USD) y el sector minorista (225 000 USD).

775 200 USD

Mediana de la cifra exigida como rescate a las instituciones educativas —superior a la mediana de 698 000 USD de la encuesta general.

La mitad de las peticiones de rescate a centros educativos ascendían a 1 millón USD o más.

Mediana de peticiones de rescate por sector



¿A cuánto ascendía el rescate exigido por los atacantes? Base: organizaciones cuyos datos fueron cifrados. n=1.141

Las tendencias interanuales tienen sus pros y sus contras. La mediana de la petición de rescate en el conjunto de la educación bajó de 976 000 USD en 2025 a 775 200 USD en 2026. Esta disminución se debió en gran parte a la educación primaria y secundaria, donde la mediana del rescate exigido bajó de 1,03 millones USD a 737 600 USD, mientras que en la educación superior pasó lo contrario, con un aumento de la mediana de 697 086 USD a 889 200 USD.

Importes de rescate

Las mayores cantidades exigidas en concepto de rescate el sector de la educación superior no se tradujeron en pagos más elevados. **Aunque se enfrentaron a mayores peticiones, la mediana del pago de rescate en el sector educativo fue inferior a la de otros sectores en la encuesta general**. La mediana del pago de rescate realizado por una institución educativa fue de 515 000 USD, por debajo de la mediana de la encuesta general, que fue de 769 000 USD.

Los pagos del sector educativo no se concentraron en el tramo más alto, pero sí incluían una mayor proporción de pagos de más de 5 millones USD. El 39 % de los pagos del sector educativo fueron de 1 millón USD o más, por debajo del 44 % registrado en la encuesta general. Sin embargo, el 23 % fueron de 5 millones USD o más, por encima del índice del 16 % de la encuesta general. Cuando el sector educativo paga, suele hacerlo con cantidades menores que otros sectores, pero una minoría significativa paga sumas muy elevadas.

Mediana del pago de rescate

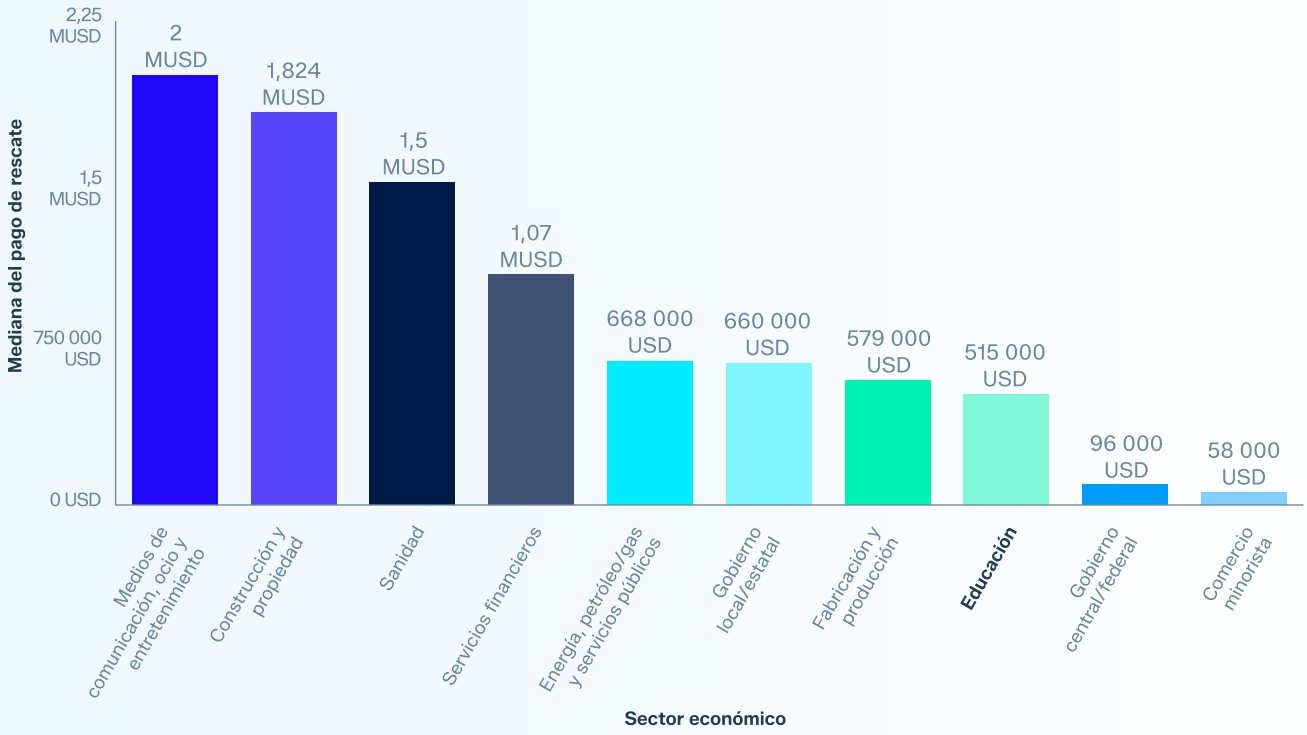
	2025	2026
Educación	0,50 MUSD (n=100)	0,52 MUSD (n=62)
Todos los sectores	1,00 MUSD (n=847)	0,77 MUSD (n=587)

¿Cuánto se pagó aproximadamente a los atacantes en concepto de rescate? Base: organizaciones que pagaron el rescate. Números base en la tabla.

515 000 USD

Mediana del rescate pagado por las instituciones educativas —inferior a la mediana de 769 000 USD de la encuesta general, a pesar de que las peticiones de rescate fueron más elevadas.

Mediana de pagos de rescate por sector



¿Cuánto se pagó aproximadamente a los atacantes en concepto de rescate? Base: organizaciones que pagaron el rescate. n=587. Excluye los sectores con menos de 30 encuestados a esta pregunta.

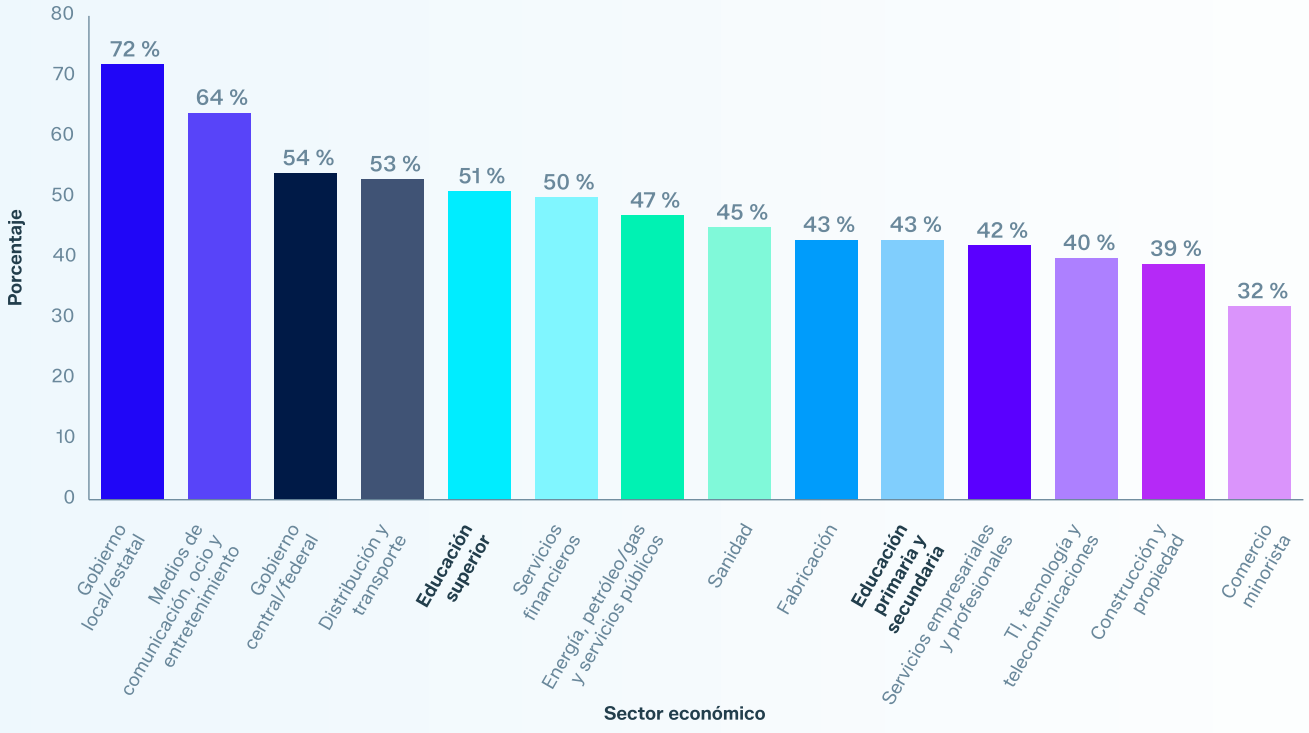
Las tendencias interanuales también fueron dispares en cuanto a los pagos de rescates. La mediana del pago de rescate en el conjunto del sector educativo se mantuvo prácticamente estable, con un ligero repunte de 500 000 USD en 2025 a 515 000 USD en 2026. La mediana del importe pagado en la educación primaria y secundaria cayó en picado durante el mismo periodo, pasando de 800 000 USD a 320 000 USD. Así pues, el ligero aumento a nivel del sector en conjunto se debió a la educación superior.

Debido a que menos de 30 instituciones de educación superior registraron una cifra de pagos este año (n=27), no podemos mostrar una línea de tendencia independiente fiable para los pagos de educación superior, por lo que recomendamos utilizar las tendencias de pago de educación combinada.

Porcentaje de organizaciones que pagaron el rescate, por sector

La propensión a pagar rescates varió entre los dos segmentos del sector educativo. El 51 % de las víctimas de la educación superior pagaron el rescate, por encima del índice general del 48 %, mientras que el 43 % de las víctimas de la educación primaria y secundaria pagaron el rescate, resistiéndose al pago con más frecuencia que la encuesta general.

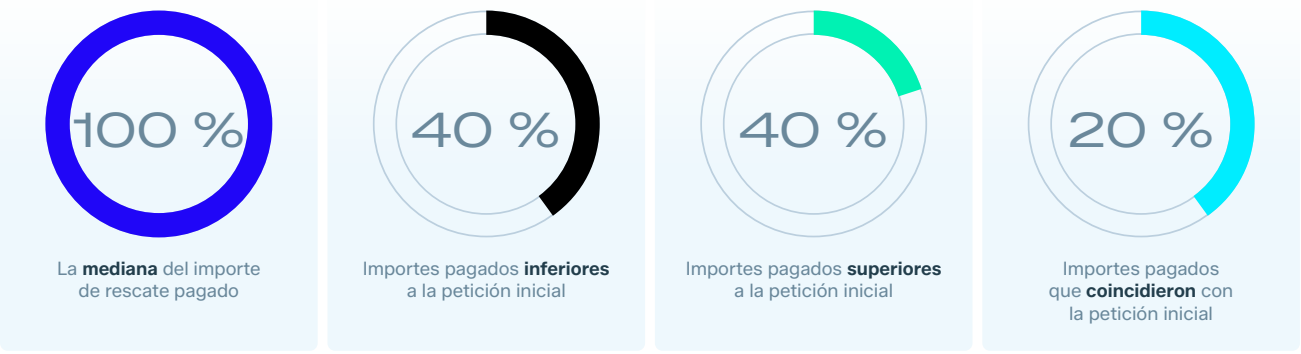
Porcentaje que pagó el rescate por sector



¿Cómo recuperó su organización los datos? Base: organizaciones cuyos datos fueron cifrados. n=1.214

Pagos reales frente a peticiones iniciales

Entre las instituciones educativas que pagaron el rescate, el 40 % pagó menos de lo que se les pidió al principio, el 40 % pagó más y el 20 % pagó exactamente lo que se les exigió. La mediana de las instituciones pagó el 100 % del importe exigido, frente al 82 % en 2025. Así que, aunque una parte importante de las instituciones consiguió rebajar el importe, otra parte igual acabó pagando más de lo que se les pidió inicialmente.



En cuanto al pago del rescate que se hizo, ¿fue inferior, igual o superior a la cantidad exigida inicialmente? Se excluyen los casos atípicos. Combina educación superior y educación primaria y secundaria. n=58.

El impacto a nivel empresarial y humano

Costes de recuperación del ransomware

El sector educativo tuvo que hacer frente a unos costes de recuperación superiores a la media. **El coste medio (media) de rectificar un ataque de ransomware, sin contar el rescate pagado, fue de 2,46 millones USD en la educación primaria y secundaria y de 1,99 millones USD en la educación superior**, ambos por encima de la media de la encuesta general: 1,7 millones USD.

La educación primaria y secundaria fue la peor parada durante dos años seguidos. Su coste medio de recuperación subió ligeramente, pasando de 2,28 millones USD en 2025 a 2,46 millones USD en 2026, lo que la convirtió en el sector educativo más caro y la situó muy por encima de la media de la encuesta general (1,7 millones USD).

Coste de recuperación medio

	2025	2026
Educación primaria y secundaria	2,28 MUSD (n=243)	2,46 MUSD (n=131)
Educación superior	0,90 MUSD (n=198)	1,99 MUSD (n=95)
Todos los sectores	1,53 MUSD (n=3400)	1,70 MUSD (n=2158)

¿Cuál fue el coste aproximado que tuvo que asumir su organización para rectificar los perjuicios del ataque de ransomware más significativo? Media, sin contar el rescate pagado. Números base en la tabla.

La educación superior es donde la brecha se amplió más marcadamente. Su coste medio de recuperación se duplicó con creces, pasando de 0,90 millones USD en 2025 a 1,99 millones USD en 2026. En el informe de 2025, la educación superior registró uno de los costes de recuperación más bajos de todos los sectores. Este año se ha acercado al de la educación primaria y secundaria. Ambos segmentos del sector educativo se sitúan ahora por encima de la media de la encuesta general, que a su vez subió ligeramente de 1,53 millones a 1,7 millones USD.

1,09 MUSD

Aumento de los costes medios de recuperación del ransomware en la educación superior de 2025 a 2026.

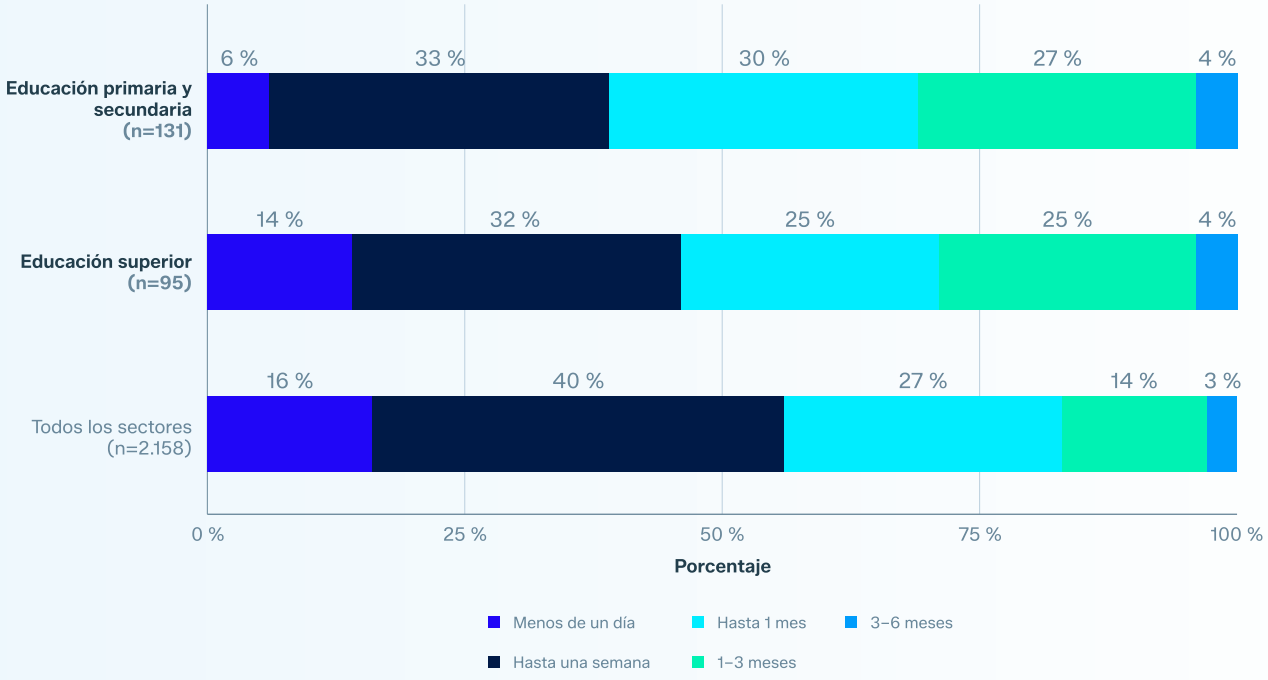
Tiempo de recuperación

Las instituciones educativas no solo pagaron más por recuperarse, sino que también tardaron más en hacerlo. La división más clara se encuentra en la franja de recuperación de uno a tres meses: El 27 % de las instituciones de educación primaria y secundaria y el 25 % de las de educación superior necesitaron tanto tiempo para recuperarse completamente, frente a solo el 14 % de la encuesta general. **La educación tenía casi el doble de probabilidades de sufrir una recuperación de un mes o más**.

31 %

La proporción de instituciones de educación primaria y secundaria que necesitaron al menos un mes para recuperarse, más que cualquier otro sector.

Cuánto tiempo tardó en recuperarse del ransomware



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

El extremo más rápido de la escala cuenta la misma historia, pero al revés. Solo el 6 % de las instituciones de educación primaria y secundaria se recuperaron en menos de un día, frente al 16 % de la encuesta general y el 14 % de la educación superior.

En ningún sector se registró una proporción mayor de recuperaciones lentas que en la educación primaria y secundaria, donde el 31 % de las instituciones tardaron al menos un mes en recuperarse por completo.

El impacto del ransomware a nivel humano

El impacto humano en el ámbito educativo fue mayor que en la encuesta general, y cada segmento del sector educativo lo percibió de forma diferente. En la educación superior, la presión más notable vino de arriba: el 53 % de los equipos señaló un aumento de la presión por parte de los altos cargos, 13 puntos por encima del índice del 40 % registrado en la encuesta general. Los cambios en el equipo o en la estructura organizativa también fueron más comunes en la educación superior (43 % frente al 32 % en todos los sectores).

La experiencia en la educación primaria y secundaria se centró en el reconocimiento y la carga de trabajo. Casi la mitad de los equipos de educación primaria y secundaria (49 %) registraron un mayor reconocimiento por parte de los directivos, por encima del índice general de encuesta del 36 %. El reconocimiento puede ser positivo, pero el aumento de la carga de trabajo no lo es. El 43 % de los que trabajan en la educación primaria y secundaria mencionaron un aumento constante de la carga de trabajo, frente al 31 % general. La atención tiene sus pros y sus contras: más visibilidad, pero también una carga más pesada y constante.

53 %

El porcentaje de equipos de TI y seguridad de la educación superior que se enfrentaron a una mayor presión por parte de los altos cargos tras un ataque, frente al 40 % en toda la encuesta.

El impacto del ransomware a nivel humano

Repercusión	Educación primaria y secundaria (n=81)	Educación superior (n=51)	Todos los sectores (n=1214)
Aumento de la ansiedad o el estrés por futuros ataques	40 %	33 %	41 %
Aumento de la presión por parte de los cargos directivos	48 %	53 %	40 %
Mayor reconocimiento por parte de los cargos directivos	49 %	29 %	36 %
Cambios en la estructura del equipo o la organización	33 %	43 %	32 %
Cambio en las prioridades o el enfoque del equipo	33 %	35 %	32 %
Sentimiento de culpa por no haber podido detener el ataque	31 %	25 %	31 %
Aumento continuo de la carga de trabajo	43 %	31 %	31 %
Bajas del personal por estrés o problemas de salud mental	40 %	39 %	29 %
Se ha sustituido a los responsables del equipo	27 %	29 %	21 %

¿Qué repercusiones ha tenido el ataque de ransomware en las personas de su equipo de TI/ciberseguridad? Base: organizaciones que sufrieron el cifrado de sus datos. Números base en la tabla.

El bienestar del personal se vio afectado en ambos segmentos del sector. El 39 % de los equipos de educación superior y el 40 % de los de educación primaria y secundaria afirmaron que el personal estuvo ausente debido a problemas de estrés o de salud mental, muy por encima del índice general de la encuesta del 29 %.

La rotación del liderazgo también fue elevada: el 29 % de los equipos de educación superior y el 27 % de los de educación primaria y secundaria vieron sustituido su liderazgo después del ataque, frente al 21 % en general.

Recomendaciones

Refuerce la seguridad de la identidad como medida de defensa contra el ransomware. Aproximadamente el 73 % de las víctimas de ransomware en el sector educativo confirmaron que su incidente de ransomware coincidió con su ataque más grave relacionado con la identidad, lo que pone de relieve el estrecho vínculo que existe entre la vulneración de la identidad y el ransomware en este sector. Las organizaciones educativas deben priorizar la detección y respuesta a amenazas relacionadas con la identidad (ITDR), aplicar la autenticación multifactor en todos los puntos de acceso y auditar periódicamente las credenciales de identidad, tanto humanas como no humanas.

Active la MFA de forma generalizada, sobre todo la MFA a prueba de phishing. La encuesta mostró que el 98 % de los proveedores educativos con compromiso de credenciales habían habilitado la MFA de alguna manera en el momento de su ataque, pero sus tasas de cifrado seguían siendo altas. La MFA por sí sola no es suficiente para detener los ataques, y debe activarse de forma integral en lugar de dejarse activada para las apps SaaS que la requieren y desactivada para los inicios de sesión VPN, las consolas de administración de firewall y las apps heredadas.

Refuerce la protección para endpoints frente a los modelos de IA de frontera. Aunque en este informe han bajado las notificaciones de vulnerabilidades explotadas, los expertos de Sophos prevén que los exploits vuelvan a aumentar, ya que a las empresas les cuesta mantenerse al día con los parches para las vulnerabilidades detectadas por la IA de frontera. Es fundamental contar con defensas sólidas en los endpoints que bloqueen automáticamente los ataques basados en exploits.

Recurra a apoyo especializado o a un servicio MDR. La falta de capacidad, habilidades y conocimientos especializados es un tema permanente en toda la educación, y especialmente grave en la educación superior, donde la falta de conocimientos internos destacó como una debilidad definitoria. Hacer frente a las amenazas potenciadas por la IA supondrá una presión aún mayor en estos ámbitos, ya que los equipos de seguridad intentarán mantenerse al día con una tecnología de IA en rápida evolución. A menos que pueda contar con total confianza con un equipo interno de operaciones de seguridad, considere la posibilidad de colaborar con un especialista externo para cubrir esa carencia, ya sea directamente con un proveedor de MDR que ofrezca cobertura 24/7, o con un proveedor de servicios gestionados. Los proveedores capaces de resolver más incidentes íntegramente mediante la IA y la automatización suponen un factor multiplicador que ayuda a subsanar las carencias en materia de conocimientos y capacidad.

Invierta en infraestructura de copias de seguridad y recuperación. La copia de seguridad fue la vía de recuperación dominante tanto para la educación primaria y secundaria como para la educación superior (77 % y 69 %, ambas por encima de la encuesta general). Las copias de seguridad deben someterse a pruebas periódicas, almacenarse fuera de línea o en formatos inmutables e integrarse en un plan de respuesta ante incidentes documentado que pueda ejecutarse en situaciones de presión.

Mantenga programas de gestión de riesgos. La explotación de vulnerabilidades sigue siendo un vector de ataque importante y es probable que aumenten a medida que los modelos de IA de frontera encuentren nuevas debilidades más rápido. Las instituciones educativas deben mantener una cadencia rigurosa en la aplicación de parches y centrarse en medidas de mitigación, como la segmentación, Zero Trust Network Access y el despliegue de la autenticación multifactor/continua.

Reduzca la exposición a través del firewall y aproveche su telemetría para detectar los ataques de forma temprana. Los datos de 2026 mostraron que los firewalls son buenos para detectar los indicios de ransomware: el 65 % disponía de datos suficientes para identificar un ataque antes de que el ransomware fuera detonado. Pero incluso en esos casos de detección temprana, las víctimas en el sector educativo seguían teniendo sus datos cifrados el 51 % de las veces, porque el firewall a menudo no puede confirmar o detener un ataque sin telemetría de otros puntos de control. Asegúrese de que el firewall reciba actualizaciones rápidas (y, a ser posible, automatizadas) y minimice los servicios expuestos a Internet, como el acceso de administrador y los portales de usuario. Conecte los firewalls a XDR y MDR para que la telemetría del firewall ayude a detectar los ataques de ransomware antes de que despliegen las cargas. Un sistema de defensa de ciberseguridad, en el que los controles compartan señales, es la respuesta.

Resumen de las medidas recomendadas:

1. Segmentación para ralentizar a los atacantes
2. ZTNA para sustituir las VPN tradicionales y contener los exploits de las aplicaciones
3. Detección y respuesta a amenazas de identidad (ITDR) para reforzar la infraestructura de identidad
4. MFA resistente al phishing como destino en lugar de como línea de partida
5. Aplicación sistemática de parches en los dispositivos conectados a Internet
6. Detección y respuesta 24/7

Conclusión

El estado del ransomware en el sector educativo 2026 revela un panorama de amenazas en transición.

Hay indicios de progreso: las peticiones de rescate están disminuyendo, la recuperación basada en copias de seguridad se ha disparado a niveles casi récord y el pago de rescates por parte de las instituciones educativas es bajo en comparación con otros sectores.

Al mismo tiempo, los retos que aún persisten son considerables. Más de la mitad de los ataques de ransomware contra el sector educativo siguen consiguiendo cifrar los datos, los costes medios de recuperación ascienden a 2,26 millones USD por incidente (una cifra superior a la encuesta general) y el sector de la educación primaria y secundaria registró el mayor porcentaje de recuperaciones que duraron un mes o más.

La identidad es donde se concentra la exposición de la educación. Un mayor porcentaje de instituciones educativas confirmó que su incidente de ransomware fue el mismo que su ataque de identidad más significativo en comparación con la encuesta general. Para un sector en el que la recuperación ya es más lenta y costosa, ese estrecho acoplamiento hace que la infraestructura de identidad sea el lugar de mayor influencia para invertir.

Las organizaciones educativas también deben prepararse para el principal reto en materia de ciberseguridad de la próxima década: las amenazas potenciadas por IA. Los datos ya dan una pista del motivo: el 62 % de las instituciones educativas citó una laguna de seguridad, conocida o desconocida, como factor determinante en el ataque que sufrieron, y el 63 % señaló la falta de personal o de conocimientos. Ambas carencias cobran mayor relevancia a medida que la IA acelera la velocidad y la magnitud de los ataques, ya que los adversarios la utilizan para detectar puntos débiles con mayor rapidez y orquestar ataques contra múltiples puntos de control a la velocidad de las máquinas.

También hay una señal más profunda en los datos de causa raíz de este año. La combinación de causas raíz parece estar equilibrándose; en todos los sectores, incluida la educación, no hay ningún factor que destaque por encima de los demás. Esto hace que centrar las defensas demasiado en una sola causa raíz sea arriesgado, porque los atacantes están logrando su objetivo a través de múltiples vectores.

El patrón de los resultados de este año, especialmente en el bajo impacto de la detección de firewall y la activación de la MFA en los resultados, apunta en una dirección coherente: cuando las defensas operan en aislamiento, no está protegido. Reducir la brecha frente a los ataques de la era de la IA dependerá menos de añadir más herramientas y más de conectar las que ya existen, de modo que el contexto, la detección y la respuesta puedan avanzar a la velocidad que las amenazas exigen actualmente.

Los proveedores de educación que obtendrán mejores resultados frente al ransomware en los próximos años serán aquellos que mantengan la atención de los directivos en este problema mientras adoptan sistemas de defensa integrados y basados en IA, invirtiendo no solo en tecnología y procesos, sino también en las personas que se encargan de hacer frente a estas amenazas cada día.

SOPHOS

Para obtener más información sobre el ransomware y cómo Sophos puede ayudarle a proteger su organización, visite nuestro sitio web.

Ventas en España
Tel.: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

2026-09-12 ES (DD)