SOPHOS
Cybersecurity evolved.

El estado del ransomware en el sector educativo 2021

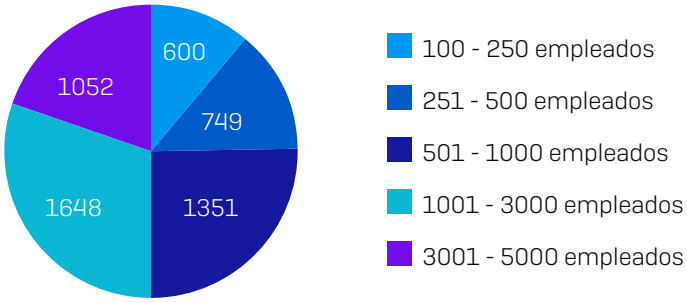
Basado en una encuesta independiente a 499 responsables de TI, este informe aporta nueva información detallada sobre la situación del ransomware en el sector educativo. Ofrece un análisis exhaustivo de la incidencia del ransomware en la educación, el impacto de los ataques, el coste de la remediación del ransomware y la proporción de datos que las organizaciones educativas pueden recuperar tras un ataque. La encuesta también revela en qué se diferencia este sector de los demás, además de las expectativas futuras y el nivel de preparación de las organizaciones educativas frente a estos ataques.

Monográficos de Sophos. Julio de 2021

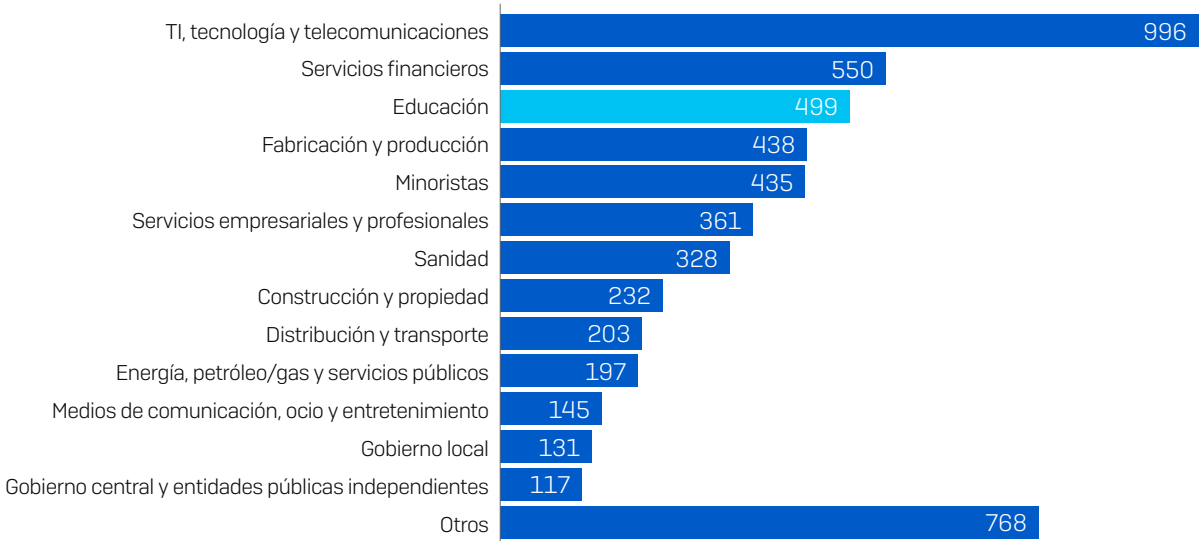
Acerca de la encuesta

Sophos encargó a la consultora independiente Vanson Bourne la realización de una encuesta a 5400 directores de TI de 30 países. Los encuestados procedían de una amplia variedad de sectores, incluidos 499 encuestados del sector educativo. La encuesta se llevó a cabo en enero y febrero de 2021.

¿Cuántos empleados tiene su organización en todo mundo? [5400]



¿A qué sector pertenece su organización? [5400]



El 50 % de los encuestados de cada país procedían de organizaciones con entre 100 y 1000 empleados y el otro 50 %, de organizaciones con entre 1001 y 5000 empleados. Los 499 responsables de TI del sector educativo procedían de todas las regiones geográficas incluidas en la encuesta: América, Europa, Oriente Medio, África y Asia-Pacífico.

Región	N.º de encuestados
América	142
Europa	138
Oriente Medio y África	85
Asia-Pacífico	134

499 responsables de TI del sector educativo

Principales conclusiones en el sector educativo

- **El 44%** de las organizaciones **se vieron afectadas por el ransomware en el último año**.
- El **58 %** de las organizaciones afectadas por el ransomware afirmaron que los ciberdelincuentes **consiguieron cifrar sus datos** en el ataque más importante.
- El **35%** de las organizaciones cuyos datos fueron cifrados **pagaron el rescate para recuperar sus datos** en el ataque de ransomware más importante.
- El **importe de rescate medio** fue de **112 435 USD**.
- Sin embargo, de media, **las organizaciones que pagaron el rescate recuperaron solo el 68 % de sus datos**, de modo que casi un tercio de los datos quedaron inaccesibles.
- La **factura total de rectificar un ataque de ransomware** en el sector educativo, teniendo en cuenta el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado y demás, **fue de 2,73 millones USD de media, la cifra más alta de todos los sectores encuestados**.
- El **55 %** de las organizaciones cuyos datos se cifraron **utilizaron copias de seguridad para recuperar los datos**.
- El **90 %** de las organizaciones educativas tienen un **plan de recuperación de incidentes de malware**.

2020 fue un año duro para la educación, ya que sufrió el mayor número de ataques de ransomware de todos los sectores (empatado con el minorista). Al mismo tiempo, el rápido cambio de la enseñanza presencial al aprendizaje online en muchos países presionó y sobrecargó de trabajo a los equipos de TI: casi tres cuartos (74 %) de los encuestados afirmaron que sus cargas de trabajo de ciberseguridad aumentaron durante 2020, la segunda cifra más alta de todos los sectores.

Frente a estos desafíos, muchas organizaciones educativas que se vieron afectadas por el ransomware pagaron el rescate para recuperar sus datos. De hecho, el sector educativo fue el tercero que más rescates pagó (35 %) después del de la energía, el petróleo/gas y los servicios públicos (43 %) y el de los gobiernos locales (42 %). Sin embargo, las organizaciones que pagaron solo recuperaron el 68 % de sus datos de media, de modo que casi un tercio quedaron inaccesibles, y solo el 11 % recuperaron todos sus datos cifrados. Dicho de otro modo, pagar el rescate no compensa.

El impacto financiero general del ransomware es incapacitante para las organizaciones educativas. La factura media de la recuperación de un ataque de ransomware es de 2,73 millones USD, la más alta con mucho de todos los sectores y un 48 % por encima de la media mundial. Es probable que esto se deba a que muchas organizaciones educativas utilizan infraestructuras de TI desfasadas y fragmentadas, mantenidas por equipos de TI con personal insuficiente. En consecuencia, al sufrir un ataque, suelen verse obligadas a reconstruirlas totalmente desde cero, lo que supone un enorme coste económico.

Las organizaciones educativas deben dar prioridad a reforzar sus defensas contra el ransomware. La inversión en infraestructuras modernas, junto con tecnologías y conocimientos de ciberseguridad, reducirán notablemente tanto el coste global como el impacto del ransomware.

La incidencia del ransomware en el sector educativo

La experiencia de la educación con el ransomware en el último año

Cuando se preguntó a los 499 encuestados del sector educativo si su organización había sido víctima del ransomware en el último año, en el sentido de que múltiples ordenadores recibieron un ataque de ransomware pero no se cifraron datos necesariamente, el 44 % dijeron que sí.

Instituciones educativas afectadas por el ransomware en el último año

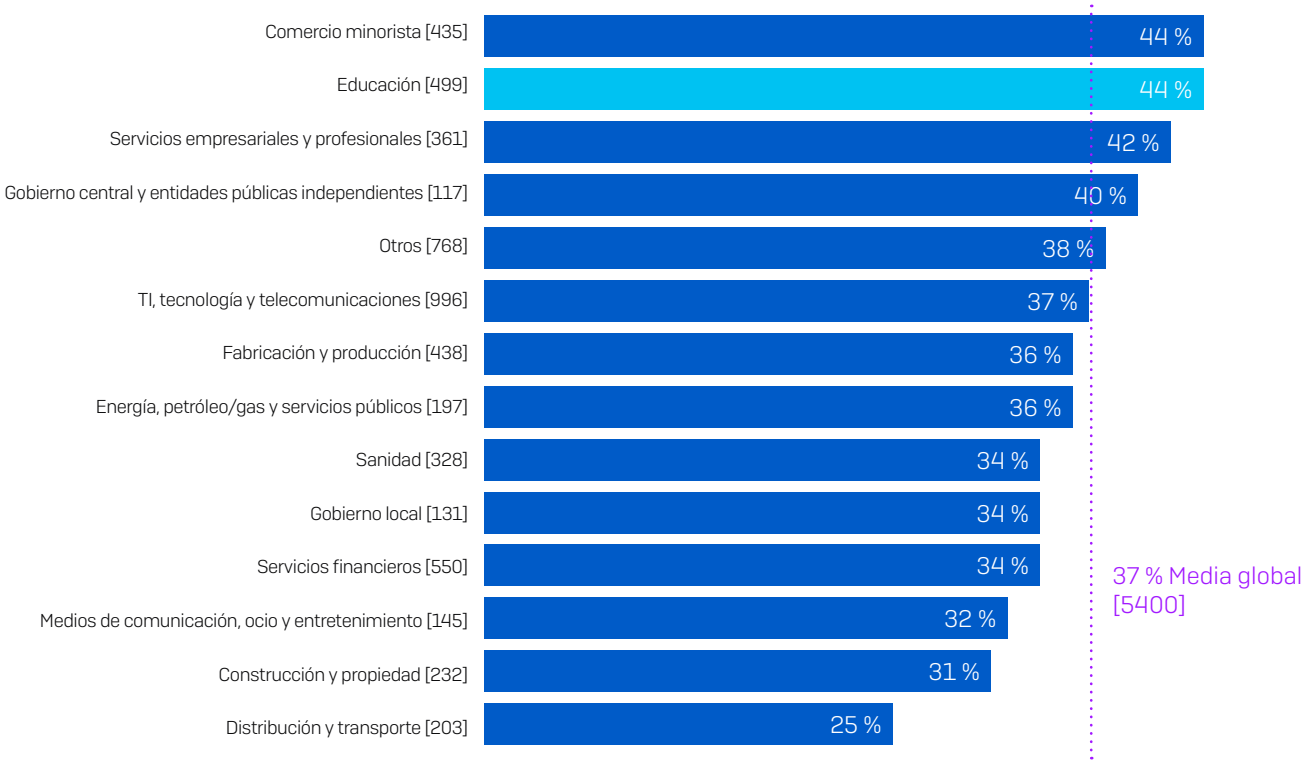
En el último año, ¿se ha visto afectada por el ransomware su organización? [499 encuestados del sector educativo]

Al mismo tiempo, el 33 % afirmaron que no habían sufrido ningún ataque en el último año pero que esperaban sufrirlo en el futuro, lo que está por debajo de la media de todos los sectores del 41 %. En cuanto al porcentaje de encuestados que no sufrieron ningún ataque y que no esperan sufrirlo en el futuro, la educación está en la línea de la media de todos los sectores del 22 %. Más adelante en el informe, exploraremos más a fondo las razones tras la expectativa de sufrir un ataque en el futuro y qué da confianza a los demás de cara a futuros ataques.

La educación registró el mayor nivel de ataques de ransomware

Si observamos la incidencia del ransomware en todos los sectores encuestados, la **educación**, junto con el **comercio minorista**, sufrieron la mayor cantidad de ataques de ransomware, ya que el 44 % de los encuestados de estos sectores afirmaron haberse visto afectados, en comparación con la media global del 37 %.

% de encuestados afectados por el ransomware en el último año



En el último año, ¿se ha visto afectada por el ransomware su organización? Sí [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por sector

El sector educativo es un blanco atractivo para los adversarios desde hace tiempo porque suele carecer de infraestructuras de TI robustas. Los presupuestos tanto para TI como para ciberseguridad son a menudo muy ajustados, y a los equipos de TI desbordados les resulta muy difícil proteger una infraestructura anticuada con herramientas y recursos limitados. Los comportamientos temerarios en Internet de los estudiantes, como descargar software pirateado, también incrementan el riesgo de ataque.

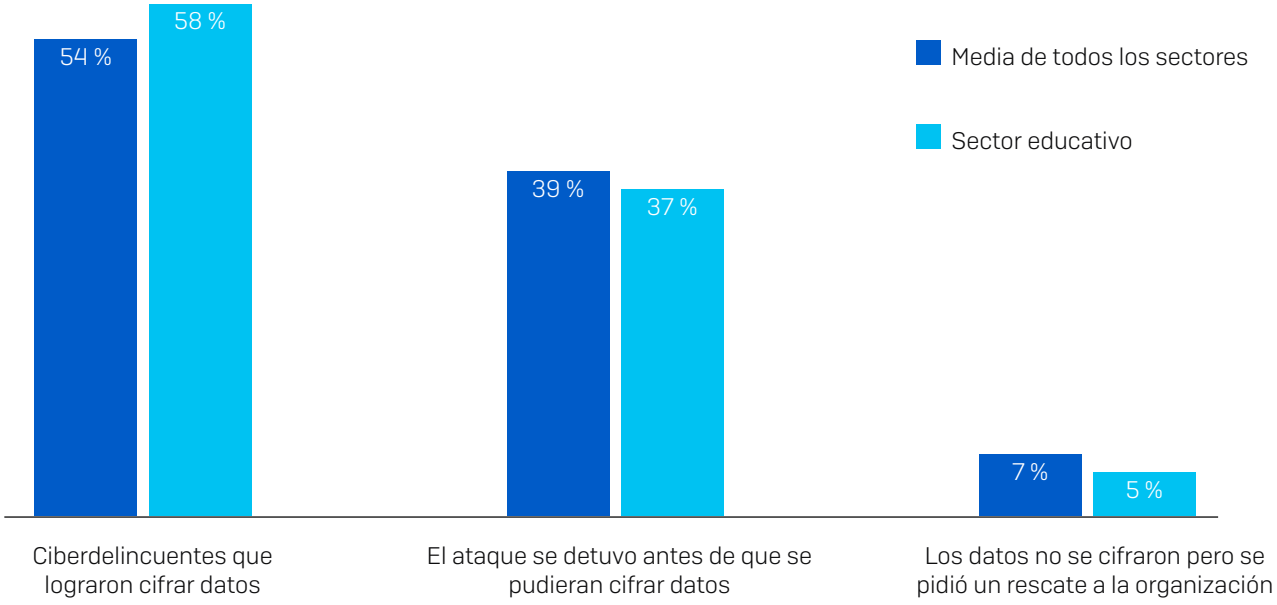
La pandemia ha agravado todavía más el desafío. Muchas instituciones educativas pasaron, sin previo aviso, de las aulas físicas a los entornos de aprendizaje remoto/virtual, lo que dio poco tiempo a los equipos de TI para planificar estrategias de seguridad o invertir en nuevas infraestructuras de TI. La rapidez del cambio también limitó las oportunidades de formación sobre ciberseguridad para profesores y estudiantes, mientras que el sobrecargado personal de TI disponía de poco tiempo para prestar soporte técnico y de seguridad.

A nivel mundial en todos los sectores, el porcentaje de organizaciones afectadas por el ransomware en el último año se redujo notablemente con respecto al año anterior, cuando el 51 % admitieron haberse visto afectadas. Si bien este descenso es una buena noticia, probablemente se debe en parte a la evolución de los comportamientos de los atacantes. Estos comportamientos han sido observados por SophosLabs y el equipo de Sophos Managed Threat Response. Por ejemplo, muchos delincuentes han pasado de los ataques automatizados, genéricos y a gran escala a ataques más dirigidos que incluyen hacking manual realizado por humanos. Si bien el número total de ataques es inferior, según nuestra experiencia, el potencial de daños de estos ataques dirigidos es muy superior.

El impacto del ransomware

Los atacantes logran cifrar los datos del sector educativo

Preguntamos a los encuestados cuyas organizaciones habían sido víctimas del ransomware, en el ataque de ransomware más importante que habían sufrido, si los ciberdelincuentes lograron cifrar sus datos.



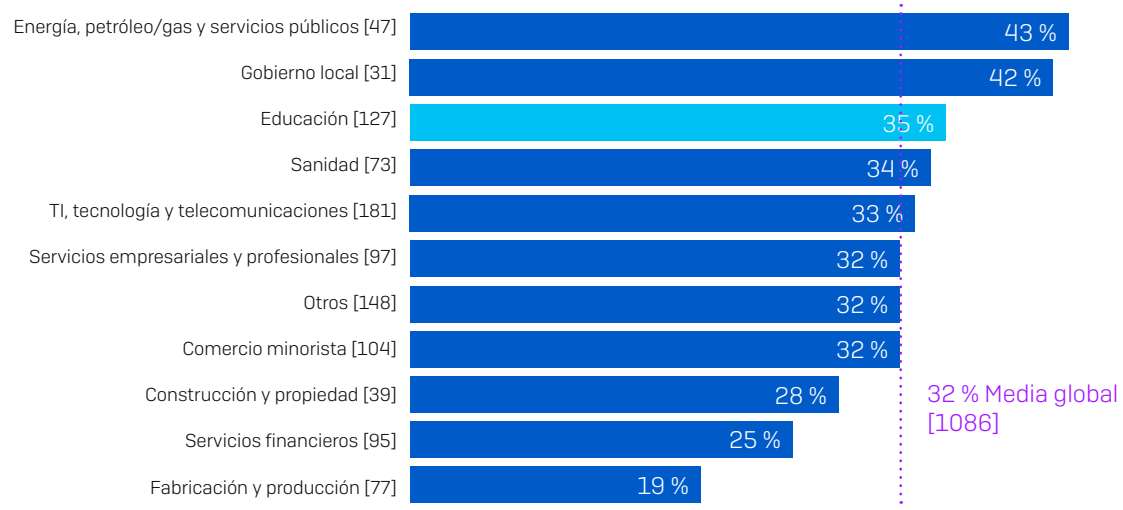
¿Consiguieron los ciberdelincuentes cifrar los datos de su organización en el ataque de ransomware más importante? [2006 encuestados de todos los sectores; 219 instituciones educativas que se habían visto afectadas por el ransomware en el último año]

La encuesta reveló que los atacantes tienen unas posibilidades de éxito para cifrar datos en el sector educativo algo superiores (58 %) a la media mundial (54 %). Las instituciones educativas también tienen menos éxito a la hora de detener el cifrado que la media mundial: un 37% frente a un 39 %. Esto probablemente se debe a la escasez de recursos de TI y a los presupuestos de TI limitados de la mayoría de las instituciones educativas. Los equipos de TI, ya con personal insuficiente, tuvieron que asumir una carga de trabajo aún mayor el año pasado cuando las aulas se convirtieron en entornos de aprendizaje virtual debido a la pandemia.

Curiosamente, el 5 % dijeron que los datos no se cifraron y aun así se pidió un rescate a la organización. En el último año, SophosLabs ha observado un aumento de los ataques de tipo extorsión en los que, en lugar de cifrar los archivos, los adversarios roban los datos y amenazan con publicarlos si no se paga el rescate. Esto requiere menos esfuerzo por parte de los atacantes, ya que no necesitan cifrar ni descifrar nada. A menudo, los adversarios se aprovechan de las sanciones oficiales por filtraciones de datos en sus exigencias a fin de presionar aún más a las víctimas para que paguen.

Predisposición a pagar el rescate

% que pagaron el rescate para recuperar sus datos



¿Su organización recuperó los datos en el ataque de ransomware más importante? Sí, pagamos el rescate; [número base en el gráfico] organizaciones en que los ciberdelincuentes lograron cifrar sus datos en el ataque de ransomware más importante, omitiendo algunas opciones de respuesta, divididas por sector

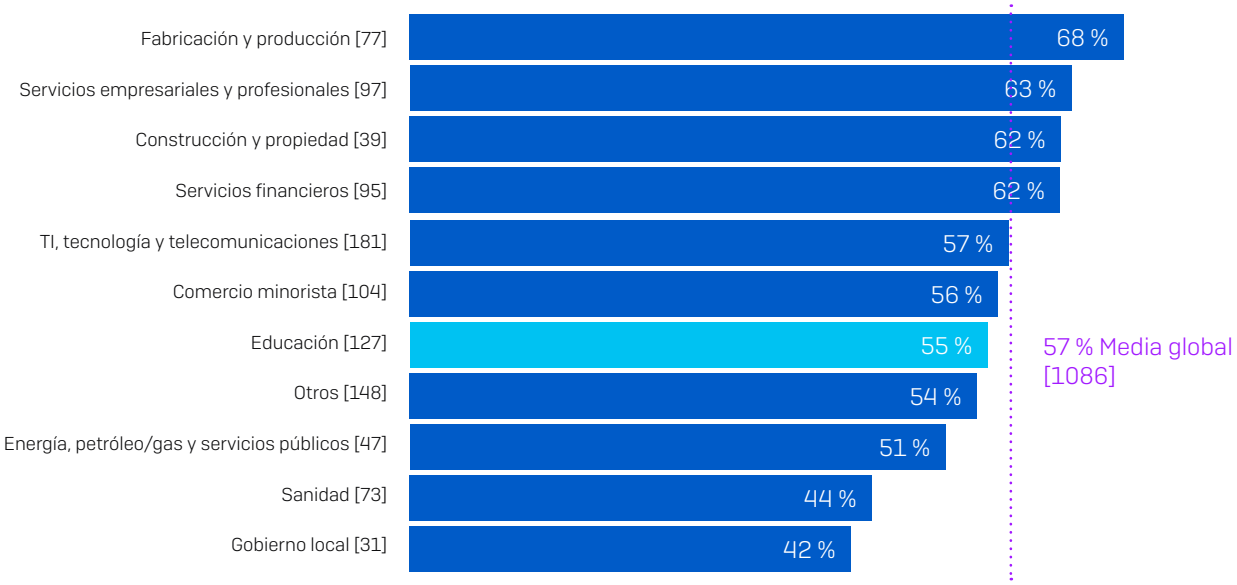
La educación es uno de los sectores más predispuestos a pagar el rescate, ya que el 35 % de los encuestados cuyos datos fueron cifrados en el ataque de ransomware más importante admitieron haber pagado el rescate frente a la media de todos los sectores del 32 %. Esto puede deberse a la presión sobre el sector educativo para garantizar la continuidad de la enseñanza, que se ha visto incrementada con la pandemia. Antes de la COVID, un ataque de ransomware contra una red educativa conllevaba un grave trastorno de la actividad lectiva. Sin embargo, cuando el aprendizaje se desarrolla mayoritariamente en plataformas virtuales, un ataque de ransomware puede significar un parón total.

De todos los sectores, el de la **energía, petróleo/gas y servicios públicos** es el más predispuesto a pagar el rescate, ya que el 43 % accedió a la demanda de un rescate. Este sector suele tener mucha infraestructura heredada que no puede actualizarse fácilmente, de modo que las víctimas podrían sentirse obligadas a pagar el rescate a fin de permitir la continuidad de los servicios.

El **gobierno local** es el sector con el segundo nivel más alto de pagos de rescates (42 %). También es el sector con más probabilidades (69 %) de que se cifren sus datos. Es muy posible que la predisposición de las entidades de gobiernos locales a pagar esté provocando que los delincuentes dirijan sus ataques más complejos y efectivos contra este colectivo.

Capacidad de restaurar datos usando copias de seguridad

% que usaron copias de seguridad para restaurar datos cifrados



¿Su organización recuperó los datos en el ataque de ransomware más importante?
Sí, usamos copias de seguridad para restaurar los datos [números base en el gráfico] organizaciones en que los ciberdelincuentes lograron cifrar sus datos en el ataque de ransomware más importante, omitiendo algunas opciones de respuesta, divididas por sector

El 55 % de los encuestados del sector educativo cuyos datos fueron cifrados durante su ataque de ransomware más importante pudieron restaurarlos a partir de copias de seguridad. Esto está en la línea de la media mundial del 57 %. Las copias de seguridad ofrecen el mejor método para restaurar los datos cifrados, por lo que las organizaciones harían bien en centrarse en este aspecto.

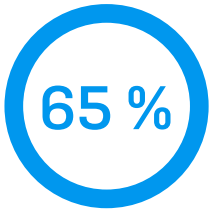
El 98 % recuperaron sus datos cifrados

Veamos ahora el porcentaje de organizaciones que pudieron recuperar sus datos después de ser cifrados.

¿Su organización recuperó los datos en el ataque de ransomware más importante? [127] Organizaciones educativas respondieron.

El 98 % de las instituciones educativas cuyos datos fueron cifrados durante su ataque de ransomware más importante los recuperaron. Solo un poco más de un tercio (35 %) pagó el rescate, el 55 % utilizó copias de seguridad y el 8 % se sirvió de otros medios para recuperar sus datos.

Pagar el rescate solo permite recuperar parte de los datos

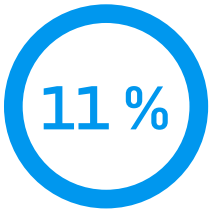


Porcentaje de datos restaurados después de pagar el rescate
MEDIA DE TODOS LOS SECTORES

Porcentaje de datos restaurados después de pagar el rescate
MEDIA DEL SECTOR EDUCATIVO

Cantidad media de datos que recuperaron las organizaciones en el ataque de ransomware más importante. [44] Organizaciones que pagaron el rescate para recuperar sus datos

De media, las instituciones educativas que pagaron el rescate recuperaron solo el 68 % de sus datos, de modo que un tercio quedó inaccesible. Esta cifra es ligeramente mejor que la media mundial (65 %), pero todavía deja inaccesible una proporción considerable de los datos.



Recuperaron TODOS sus datos

Recuperaron la mitad o menos de sus datos

Cantidad media de datos que recuperaron las organizaciones educativas en el ataque de ransomware más importante. [44] Organizaciones que pagaron el rescate para recuperar sus datos

De hecho, solo el 11 % de las organizaciones educativas que pagaron el rescate recuperaron todos sus datos, y el 32 % recuperaron la mitad o menos de sus datos. Es evidente que pagar no compensa.

El coste del ransomware

Revelamos los importes de los rescates pagados

De los 357 encuestados de todos los sectores que afirmaron que su organización había pagado el rescate, 282 también revelaron el importe exacto pagado, incluidos 37 del sector educativo.

170 404 USD
Importe de rescate medio GLOBAL

112.435 $
Importe de rescate medio en el sector EDUCATIVO

¿Cuál fue el importe del rescate que pagó su organización en el ataque de ransomware más importante?
[282/37] organizaciones que pagaron el rescate para recuperar sus datos

De forma global en todos los sectores, el importe de rescate medio fue de 170 404 USD. Sin embargo, en la educación, el pago del rescate medio fue de casi 58 0000 USD menos, situándose en 112 435 USD. Estas cifras difieren mucho de los pagos de ocho cifras que suelen verse en los titulares por varias razones.

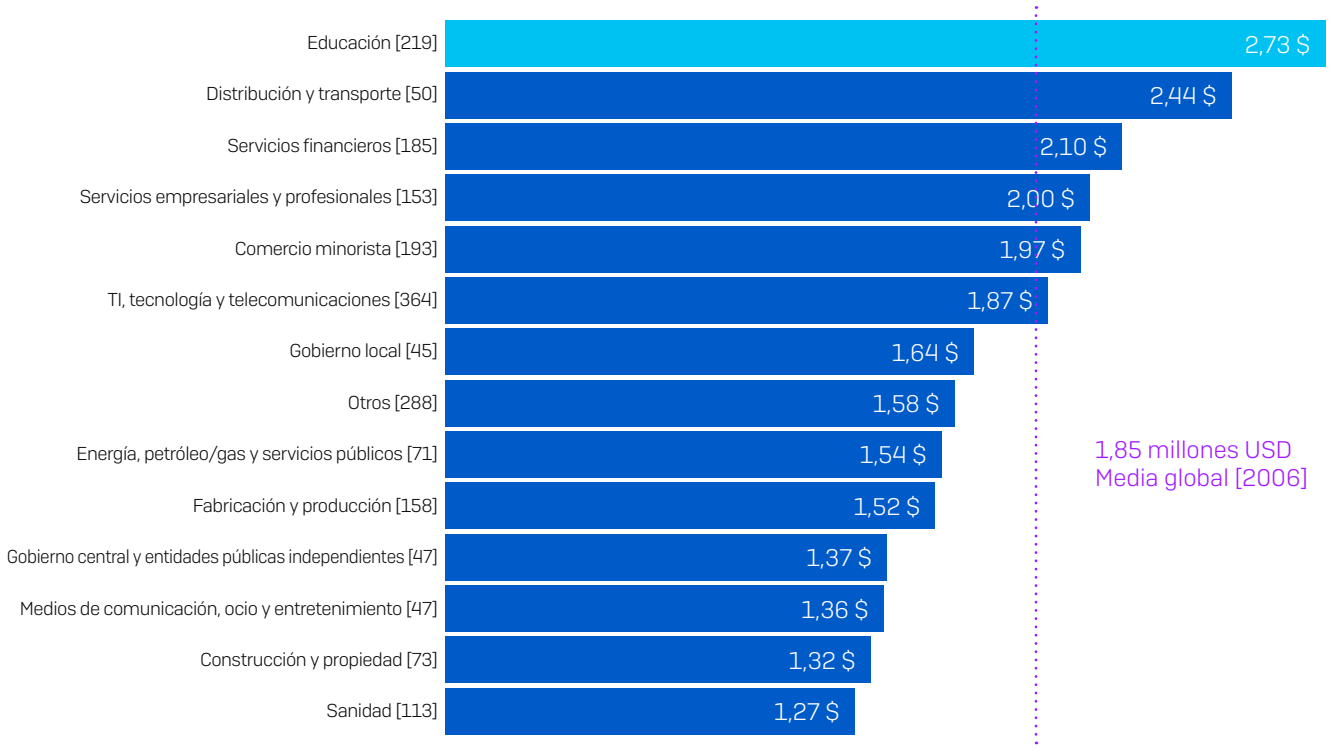
1. **Tamaño de la organización.** Nuestros encuestados pertenecen a organizaciones medianas de entre 100 y 5000 usuarios que, en general, tienen menos recursos financieros que las organizaciones de mayor tamaño. Los responsables del ransomware adaptan los rescates que exigen a la capacidad de pago de sus víctimas, por lo que normalmente aceptan importes menores de organizaciones más pequeñas. Los datos lo demuestran, ya que el rescate medio para organizaciones de 100 a 1000 empleados fue de 107 694 USD, mientras que el rescate medio pagado por las organizaciones de 1001 a 5000 empleados asciende a 225 588 USD.

2. **Tipo de ataque.** Hay muchos responsables del ransomware y muchos tipos de ataques de ransomware, desde atacantes altamente cualificados que utilizan tácticas, técnicas y procedimientos (TTP) sofisticados que se centran en objetivos individuales, hasta operadores menos habilidosos que utilizan ransomware "listo para usar" y un enfoque genérico de ataque "spray and pray". Los atacantes que realizan una gran inversión en un ataque dirigido exigen un elevado rescate que compense su esfuerzo, mientras que los responsables de ataques genéricos suelen aceptar un menor retorno de la inversión (ROI).

3. **Ubicación.** Como hemos visto al comienzo, esta encuesta cubre 30 países de todo el mundo, con distintos niveles de PIB. Los atacantes exigen los rescates más altos en economías occidentales desarrolladas, basándose en su percepción de que pueden pagar sumas mayores. Los dos importes de rescate más elevados fueron mencionados por encuestados de Italia. En cambio, en la India, el rescate medio fue de 76 619 USD, menos de la mitad de la cifra global (base: 86 encuestados).

La educación incurre en los costes de recuperación del ransomware más altos

El rescate es solo una pequeña parte del coste total de la recuperación de un ataque de ransomware. Las víctimas se enfrentan a una amplia variedad de gastos adicionales, como el coste de reconstruir y proteger sus sistemas de TI, gastos de relaciones públicas y de análisis forenses.



Coste medio aproximado para las organizaciones de rectificar las consecuencias del ataque de ransomware más reciente [considerando el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, etc.]; [números base en el gráfico] encuestados cuya organización se había visto afectada por el ransomware en el último año, divididos por sector, millones de USD

La encuesta reveló que el sector educativo incurre en los costes de recuperación d el ransomware más altos de todos los sectores, con un coste de remediación medio de su ataque de ransomware más reciente de 2,73 millones USD (considerando el tiempo de inactividad, las horas perdidas, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado, etc.). Esto es un descomunal 48 % más que la media mundial (1,85 millones USD). El frágil estado de las infraestructuras de TI del sector educativo es probablemente uno de los factores que más contribuyen a este elevado coste, ya que a menudo las organizaciones necesitan reconstruir sus sistemas de TI desde cero tras un ataque.

Este dato reafirma la importancia de invertir en la actualización de los sistemas de TI y tecnologías de ciberseguridad antes y no después de un ataque.

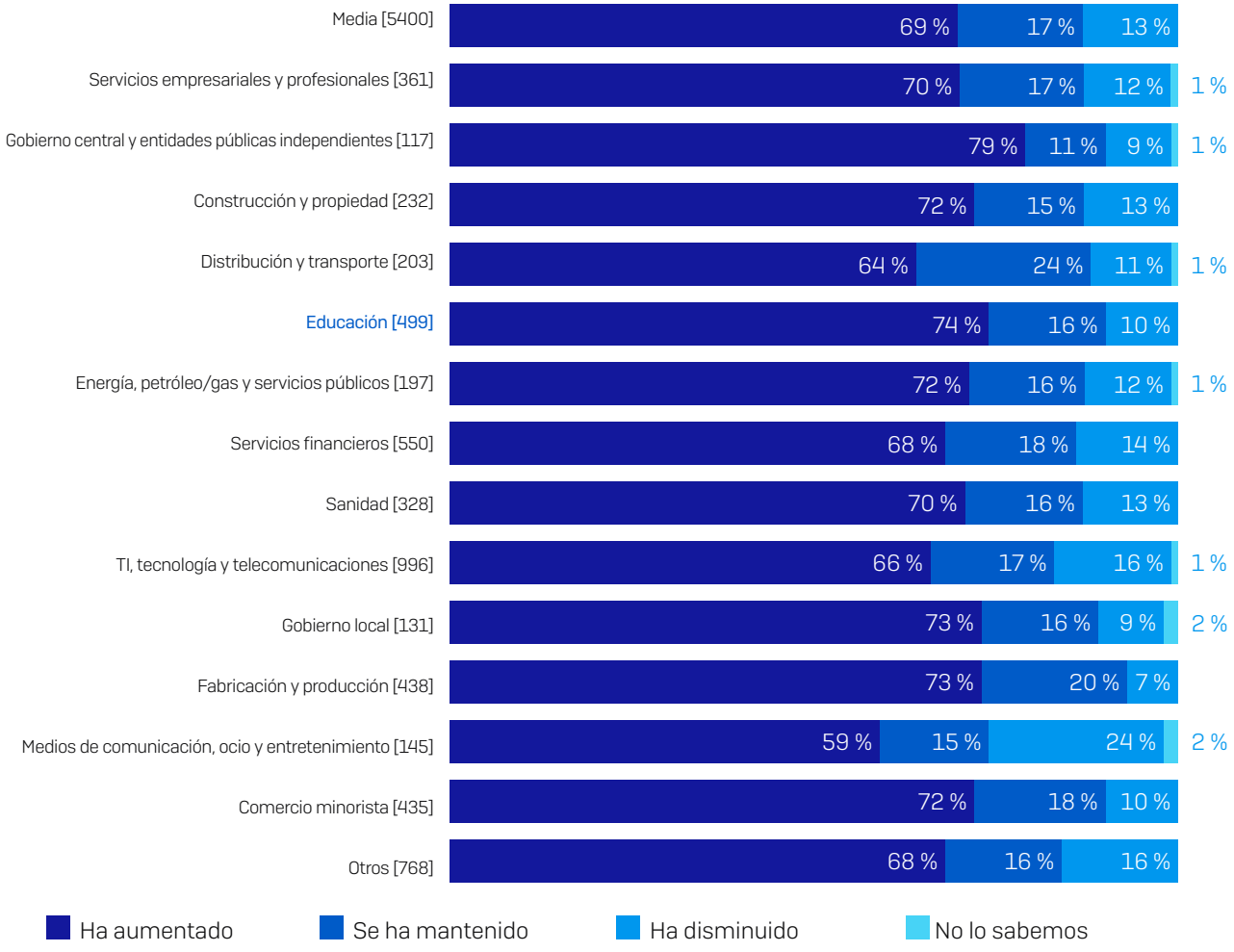
El ransomware es solo una parte del reto de la ciberseguridad

El ransomware es un importante problema de ciberseguridad para las organizaciones educativas, pero no es el único. Los equipos de TI hacen malabarismos para tratar de satisfacer múltiples demandas de ciberseguridad, y este reto se ha visto agravado por la pandemia.

La carga de trabajo en ciberseguridad ha aumentado en 2020

Preguntamos a los encuestados cómo cambió su carga de trabajo en ciberseguridad a lo largo de 2020.

Cómo ha cambiado la carga de trabajo en ciberseguridad durante 2020



Durante 2020, nuestra carga de trabajo en ciberseguridad ha disminuido/aumentado/se ha mantenido igual [números base en el gráfico], dividida por sector.

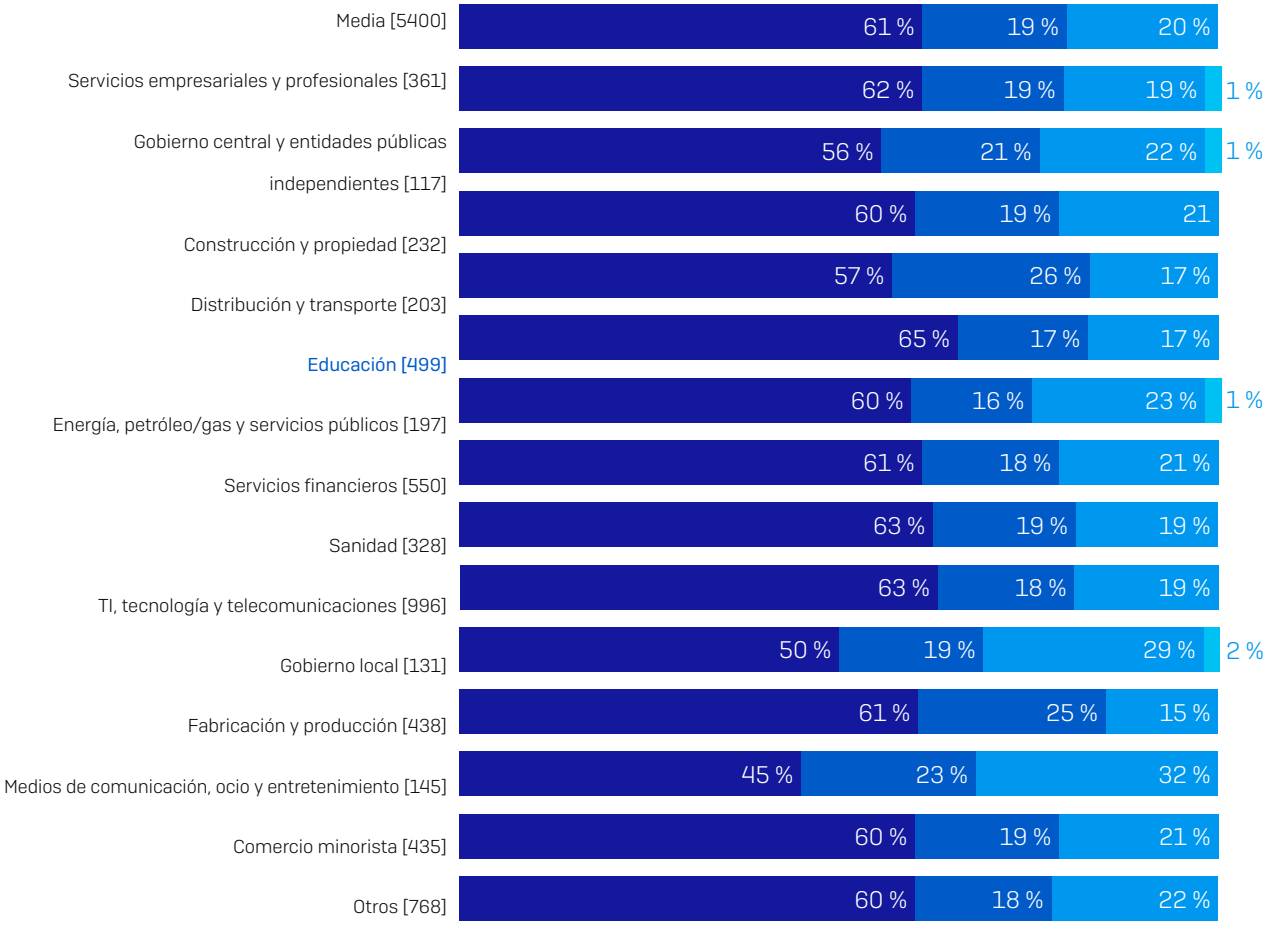
Los equipos de TI del sector educativo fueron de los que más se vieron afectados por la pandemia: el 74 % experimentaron un aumento de la carga de trabajo de ciberseguridad durante el transcurso de 2020. La mayoría de los encuestados de todos los sectores registraron un incremento, pero solo el sector del gobierno central registró un mayor crecimiento de la carga de trabajo que el sector educativo.

El cambio al aprendizaje online fue probablemente un factor clave en el incremento de la carga de trabajo. Los equipos de TI necesitaban proteger las nuevas plataformas de aprendizaje, además de los dispositivos utilizados por estudiantes y formadores. El mayor uso de dispositivos personales para enseñar y aprender acentuó aún más el reto, ya que los equipos de TI tuvieron que mitigar los riesgos de las aplicaciones peligrosas o desactualizadas que de otra forma podían convertirse en un punto de entrada para los atacantes.

El hecho de tener que centrarse sobre todo en proteger la enseñanza y el aprendizaje online seguramente redujo la capacidad de los equipos de TI para supervisar las amenazas de ransomware y responder a ellas.

El incremento de la carga de trabajo ralentizó los tiempos de respuesta

Una de las consecuencias del aumento de la carga de trabajo de ciberseguridad durante 2020 fue la ralentización del tiempo de respuesta a los casos de TI.



Durante 2020, nuestro tiempo de respuesta a los casos de TI ha disminuido/aumentado/se ha mantenido igual. [números base en el gráfico], dividido por sector. N.B. Por motivos de redondeo, algunos totales son superiores al 100 %.

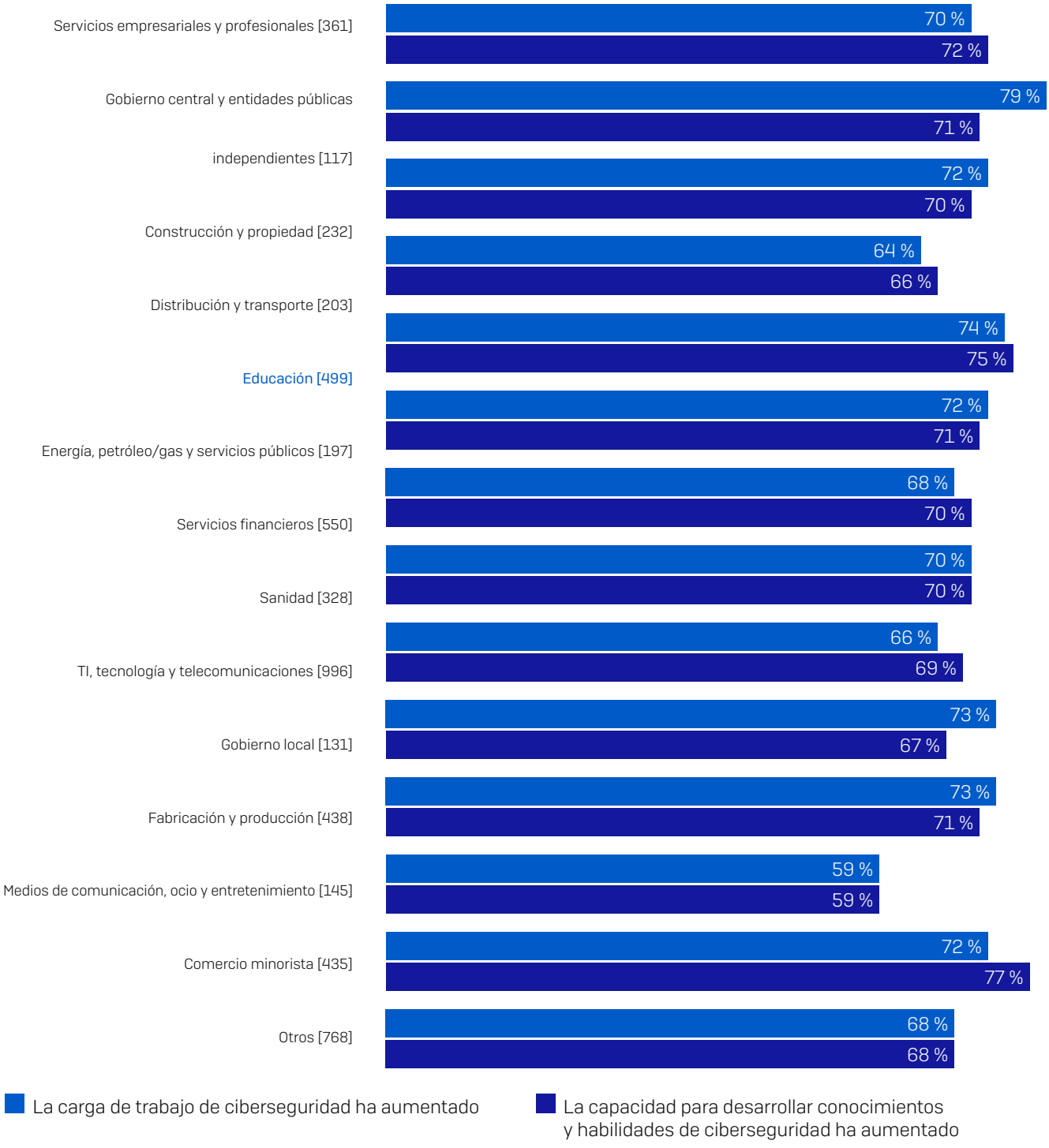
El sector educativo fue el más afectado, ya que casi dos tercios (65 %) afirmaron que el tiempo de respuesta aumentó en el último año, una de las cifras más altas de todos los sectores.

Cuando un adversario se encuentra en su entorno, es imperativo detenerlo lo antes posible. Cuanto más tiempo se le permita explorar su red y acceder a sus datos, mayor será el impacto financiero y operativo del ataque. La ralentización del tiempo de respuesta es por lo tanto un motivo de alarma.

El aumento de la carga de trabajo incrementó conocimientos y habilidades

No hay mal que por bien no venga. También existe una relación entre el aumento de la carga de trabajo en ciberseguridad y el aumento de la capacidad para desarrollar conocimientos y aptitudes en ciberseguridad.

Aumento de la carga de trabajo en ciberseguridad y aumento de la capacidad para desarrollar conocimientos y habilidades de ciberseguridad



Durante 2020, ha aumentado nuestra carga de trabajo de ciberseguridad/nuestra capacidad para desarrollar más nuestros conocimientos y habilidades de ciberseguridad [números base en el gráfico], dividido por sector

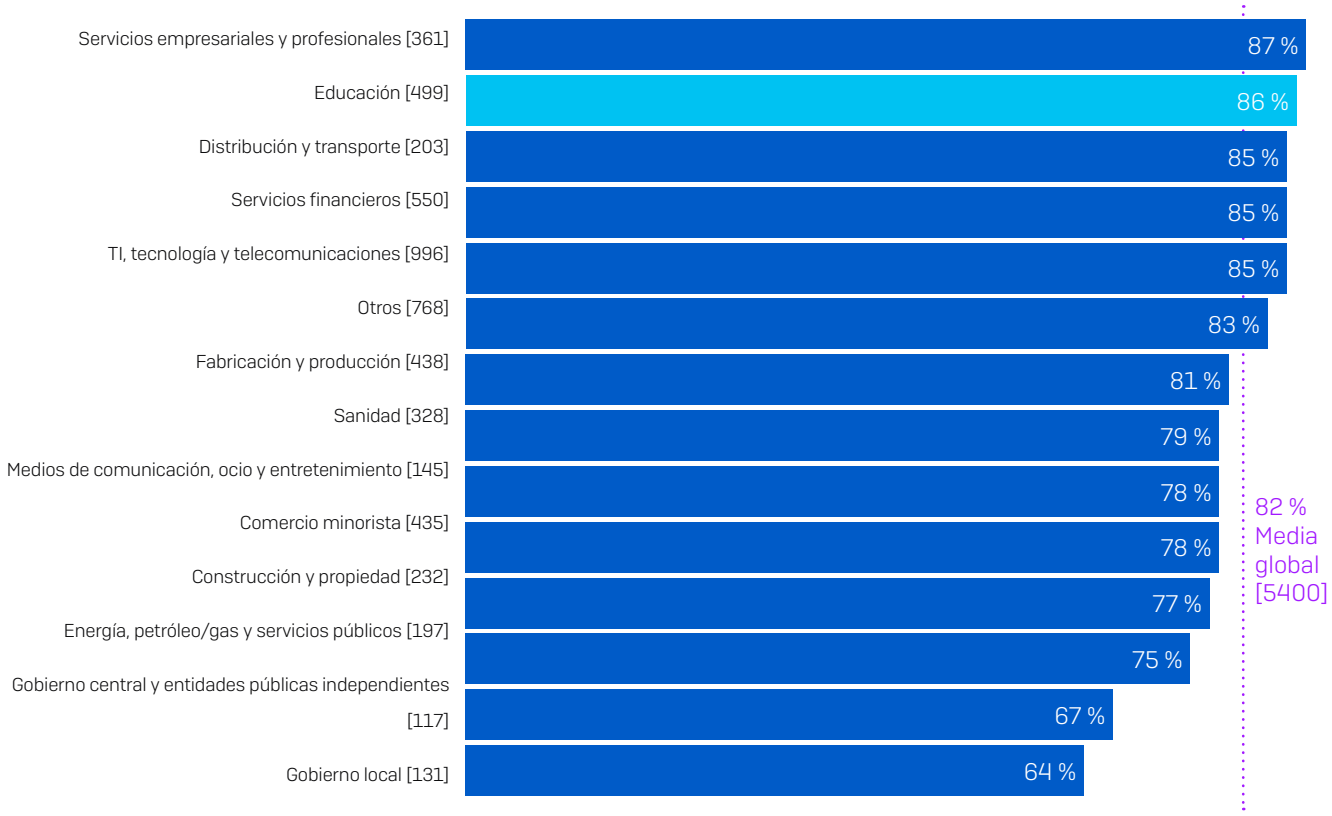
El 75 % de los equipos de TI del sector educativo manifestaron que su capacidad para desarrollar conocimientos y habilidades en materia de ciberseguridad aumentó durante 2020, la segunda cifra más alta después del sector minorista (77 %).

Si bien una mayor carga de trabajo añade presión, también ofrece más oportunidades para aprender cosas nuevas. Además, es probable que las circunstancias únicas de la pandemia también obligaran a los equipos de TI a ofrecer un rendimiento que nunca antes se les había requerido.

Nivel de preparación para asumir futuros retos

Tener las herramientas y los conocimientos adecuados es clave para poder investigar y remediar las ciberamenazas.

Tienen las herramientas y los conocimientos necesarios para investigar la actividad sospechosa



Si detecto actividades sospechosas en mi organización, tengo las herramientas y los conocimientos que necesito para investigar a fondo: Muy de acuerdo, De acuerdo. Omitiendo algunas opciones de respuesta [números base en el gráfico], divididas por sector

Teniendo en cuenta el elevado nivel de ataques de ransomware que sufrió el sector educativo y el incremento de la carga de trabajo de ciberseguridad, resulta alentador que el 86 % de los encuestados del sector educativo afirmen que disponen de las herramientas y los conocimientos que necesitan para investigar a fondo las actividades sospechosas. Esta cifra es un poco más alta que la media mundial (82 %), y lo sitúa en segundo lugar justo después de los **servicios empresariales y profesionales (87 %)**.

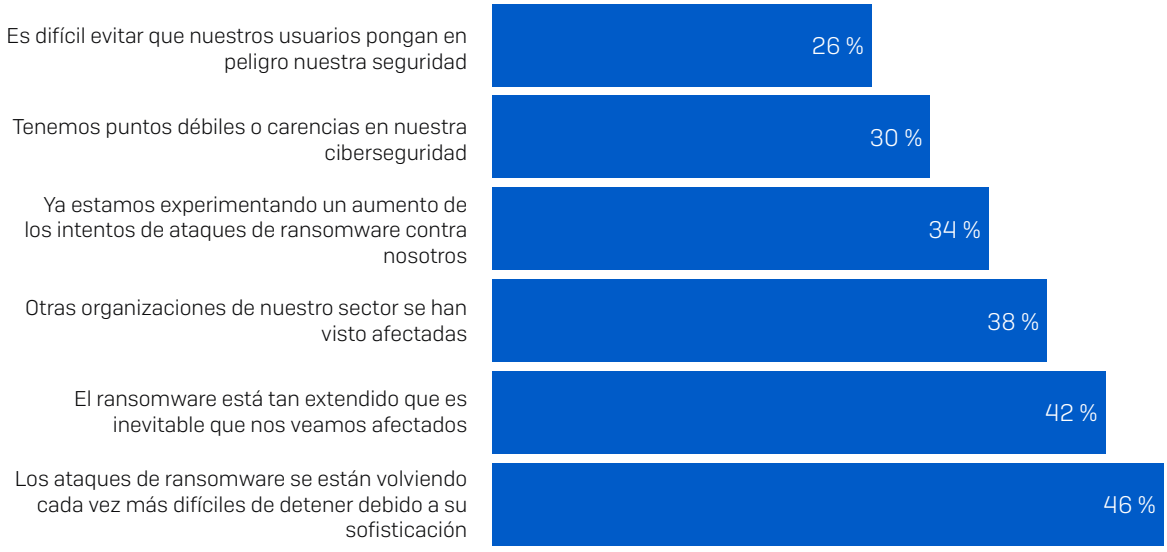
El futuro

Expectativas del sector educativo frente a futuros ataques

Al principio hemos visto que el 55 % de los encuestados del sector educativo no se vieron afectados por el ransomware el año pasado. Casi dos tercios (61 %) esperan sufrir ataques de ransomware en el futuro. En cambio, el 39 % no prevén ningún ataque.

Por qué prevé ataques el sector educativo

Entre las instituciones educativas que no fueron víctimas del ransomware pero que esperan serlo en el futuro, la razón más común (46 %) es que los ataques de ransomware se están volviendo cada vez más difíciles de detener debido a su sofisticación.



¿Por qué espera que su organización sea atacada por el ransomware en el futuro? [167 organizaciones educativas que no han sido atacadas por el ransomware en el último año pero que esperan serlo en el futuro, omitiendo algunas opciones de respuesta]

Aunque este número es elevado, el hecho de que estas organizaciones estén alerta ante la posibilidad de que el ransomware se vuelva más avanzado es algo positivo, y es probable que sea un factor que ha contribuido a que hayan logrado bloquear posibles ataques de ransomware durante el último año.

Además, el 42 % de los encuestados afirmaron que el ransomware estaba demasiado extendido como para no verse afectados.

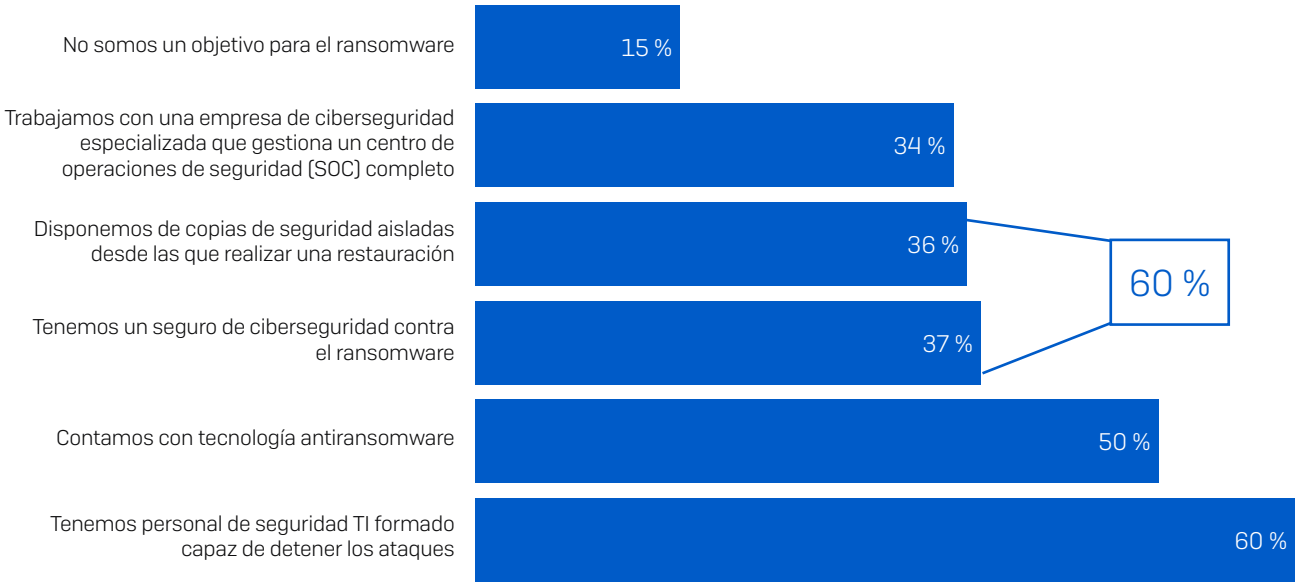
El 26 % de los encuestados ven el hecho de que los usuarios comprometan la seguridad como uno de los principales factores para sufrir un ataque de ransomware en el futuro. Resulta alentador observar que, frente a los atacantes sofisticados, la mayoría de los equipos de TI no eligen la opción fácil de culpar a sus usuarios.

De forma similar, el 30 % de los encuestados del sector educativo admiten tener puntos débiles o carencias en su ciberseguridad. Aunque lógicamente no es nada bueno tener carencias de seguridad, reconocer que estos problemas existen es un importante primer paso para mejorar las defensas.

Por qué el sector educativo no prevé ataques de ransomware

109 encuestados del sector educativo dijeron que su organización no había sufrido ataques de ransomware en el último año y que no esperan sufrir ninguno en el futuro.

Por qué los encuestados no esperan sufrir ataques de ransomware en el futuro



¿Por qué no espera que su organización sea atacada por el ransomware en el futuro? [109] instituciones educativas que no han sido atacadas por el ransomware en el último año y no esperan serlo en el futuro, omitiendo algunas opciones de respuesta

El factor más común tras esta confianza es que han formado a personal de TI para que sea capaz de detener los ataques (60 %), seguido del uso de tecnología antiransomware (50 %). Asimismo, el 34 % de los encuestados del sector educativo que no esperan ser atacados por el ransomware trabajan con una empresa de ciberseguridad especializada que gestiona un centro de operaciones de seguridad (SOC) completo.

Si bien las tecnologías avanzadas y automatizadas son elementos fundamentales de una defensa antiransomware efectiva, detener los ataques manuales también requiere una monitorización e intervención humanas por parte de profesionales cualificados. Ya sean empleados en plantilla o profesionales subcontratados, solo los expertos humanos pueden identificar algunos de los indicios de que los atacantes del ransomware le tienen en el punto de mira. Recomendamos encarecidamente a todas las organizaciones que refuercen sus conocimientos humanos ante la amenaza continuada del ransomware.

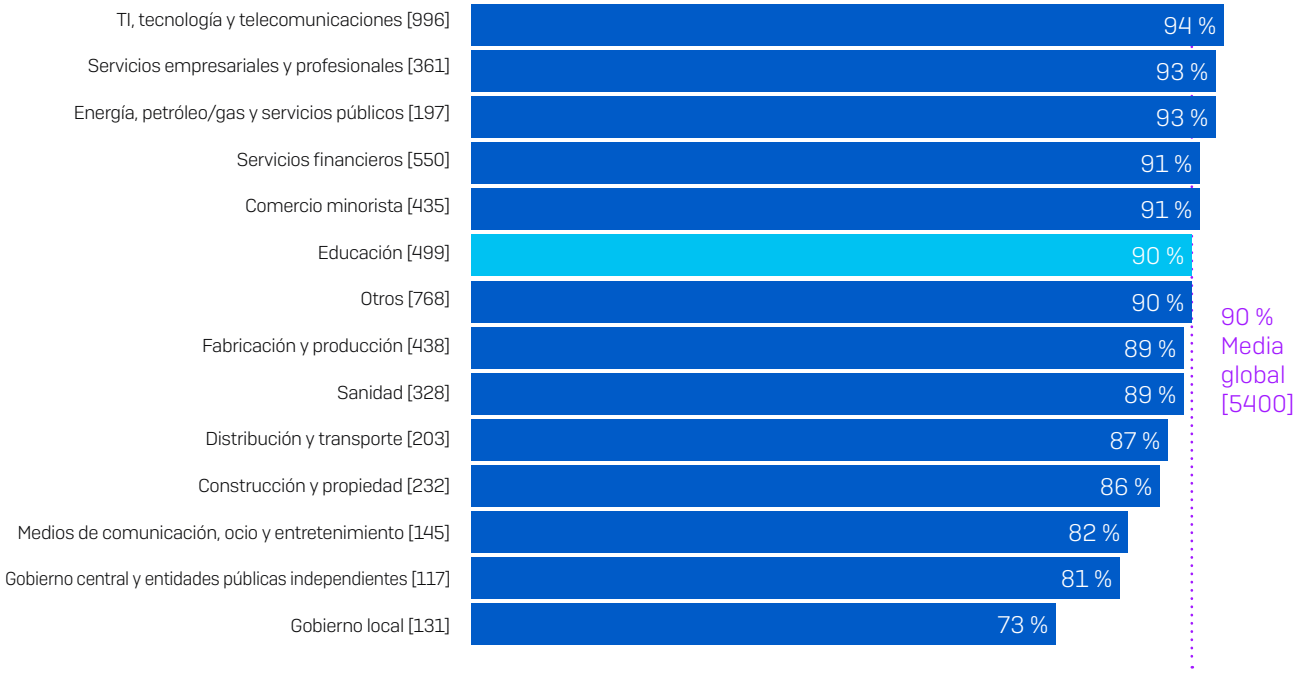
No todo son buenas noticias. Algunos resultados son preocupantes:

- El 60 % de los encuestados del sector educativo que no esperan sufrir ningún ataque depositan su confianza en enfoques que no ofrecen ninguna protección contra el ransomware.
  - El 37 % citaron un ciberseguro contra el ransomware. Los seguros ayudan a cubrir el coste de lidiar con un ataque, pero no evitan que el ataque se produzca.
  - El 36 % citaron copias de seguridad aisladas. Aunque las copias de seguridad son herramientas valiosas para restaurar los datos después de un ataque, no evitan el ataque en sí.
    N. B. Algunos encuestados seleccionaron las dos opciones anteriores, y el 60 % seleccionaron al menos una de estas dos opciones.
- El 15 % creen que no son un objetivo para el ransomware. Lamentablemente, esto no es así. Ninguna organización está a salvo.

Las instituciones educativas están bien preparadas

Responder a un ciberataque o incidente crítico puede ser increíblemente estresante. Aunque nada puede aliviar por completo el estrés que supone lidiar con un ataque, contar con un plan de respuesta a incidentes efectivo es una forma segura de minimizar el impacto.

Tienen un plan para recuperarse de un incidente de malware importante



¿El plan de continuidad empresarial o plan de recuperación de desastres de su organización incluye planes para recuperarse de un incidente de malware importante? Sí, tenemos un plan de recuperación de incidentes de malware completo y detallado, y Sí, tenemos un plan de recuperación de incidentes de malware parcialmente desarrollado; [números base en el gráfico], omitiendo algunas opciones de respuesta, divididas por sector

Por esta razón, resulta alentador descubrir que el 90 % de las instituciones educativas cuentan con un plan de recuperación de incidentes de malware: algo más de la mitad (51 %) tienen un plan completo y detallado, mientras que el 39 % tienen un plan parcialmente desarrollado. Estas estadísticas están totalmente alineadas con las cifras medias de todos los sectores.

Recomendaciones

En vista de los resultados de la encuesta, los expertos de Sophos recomiendan las siguientes prácticas para las organizaciones de todos los sectores:

1. **Dé por hecho que sufrirá un ataque**. El ransomware sigue estando muy extendido. No hay ningún sector, país ni organización a salvo del riesgo. Es mejor prepararse y no sufrir ningún ataque que lo contrario.

2. **Realice copias de seguridad**. Las copias de seguridad son el principal método utilizado por las organizaciones para recuperar sus datos tras un ataque. Y como ya hemos visto, incluso si paga el rescate, rara vez conseguirá recuperar todos sus datos, así que depende de las copias de seguridad en cualquiera de los casos.

Una sencilla regla mnemotécnica para las copias de seguridad es "3-2-1". Debería tener al menos tres copias distintas (la que esté usando en el momento actual, más dos o más aparte), utilizar al menos dos sistemas de copia de seguridad diferentes (por si uno le falla) y tener al menos una copia almacenada sin conexión y preferiblemente en una ubicación externa (donde los delincuentes no puedan manipularla durante un ataque).

3. **Despliegue una protección por capas.** Ante el importante aumento de los ataques basados en la extorsión, es más importante que nunca mantener a los adversarios fuera de su entorno como primera medida. Utilice una protección por capas para bloquear a los atacantes en tantos puntos como sea posible dentro de su entorno.

4. **Combine expertos humanos y tecnología antiransomware.** Una de las claves para detener el ransomware es una defensa exhaustiva que combine una tecnología antiransomware dedicada y la búsqueda de amenazas realizada por humanos. La tecnología le brinda el alcance y la automatización que necesita, mientras que los expertos humanos están más capacitados para detectar las tácticas, técnicas y procedimientos que indican que un atacante habilidoso está intentando infiltrarse en su entorno. Si no dispone de las capacidades en plantilla, plantéese la opción de contratar a una empresa especializada en ciberseguridad para que le ayude. Ahora los SOC son opciones realistas para las organizaciones de todos los tamaños.

5. **No pague el rescate.** Sabemos que esto es fácil de decir pero mucho menos fácil de hacer cuando la actividad de su organización se encuentra interrumpida a causa de un ataque de ransomware. Con independencia de cualquier consideración ética, pagar el rescate no es una forma efectiva de recuperar sus datos. Si opta por pagar, asegúrese de incluir en su análisis de costes y beneficios la expectativa de que los adversarios restaurarán, de media, solo dos terceras partes de sus archivos.

6. **Tenga un plan de recuperación del malware.** La mejor manera de evitar que un ciberataque acabe en una infracción de seguridad es prepararse con antelación. Las organizaciones que sufren un ataque a menudo se dan cuenta de que podrían haber evitado muchos costes, molestias e interrupciones si hubieran contado con un plan de respuesta a incidentes.

Más recursos

La Guía de respuesta a incidentes de Sophos ayuda a las organizaciones a definir el marco de su plan de respuesta a incidentes de ciberseguridad y explica los 10 principales pasos que debe incluir su plan.

A los responsables de la seguridad también puede interesarles consultar el artículo Cuatro consejos clave de los expertos en respuesta a incidentes, que pone de relieve las principales lecciones que todo el mundo debería aprender en lo que respecta a responder a incidentes de seguridad.

Ambos recursos se basan en experiencias del mundo real de los equipos de Sophos Managed Threat Response y Sophos Rapid Response, que han respondido de forma conjunta a miles de incidentes de ciberseguridad.

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.

05-07-2021 (SB-NP)

SOPHOS