SECTOR
ASEGURADOR

OCTUBRE 2025

INFORME 2025

CIBERSEGURIDAD EN EL SECTOR DE LA EDUCACIÓN

Análisis completo de los principales retos y cómo mejorar la resiliencia cibernética.

Creado por:
JOSÉ ROMERO SALVADOR

INSURANCE AREA CORREDURÍA DE SEGUROS SL.
www.sectoraseguradores.es
comercial@sectoraseguradores.es
(+34) 91 00 545 00

Contexto sobre este informe

Este informe busca ofrecer una visión clara y accionable del riesgo real al que se exponen los centros educativos y universidades, conectando amenazas con consecuencias operativas, legales y reputacionales.

Esperamos que permita entender la importancia de la ciberseguridad de cara a tener un nivel de protección adecuado a la exposición del sector educativo, justificar las decisiones de equipos directivos, y poder alinear expectativas.

En definitiva, es una guía práctica para pasar de la intuición a un plan de ciberseguridad medible, realista y adaptado al contexto de la ciberseguridad que necesita el sector educativo español.

Creado por:
JOSÉ ROMERO SALVADOR

INSURANCE AREA CORREDURÍA DE SEGUROS SL.
www.sectoraseguradores.es
comercial@sectoraseguradores.es
(+34) 91 00 545 00

Reflexión del CEO

José Romero - Ingeniero Informático

“Aquellos que tienen el privilegio de saber, tienen la obligación de actuar”
Albert Einstein

Los profesionales que nos dedicamos a la ciberseguridad, vivimos y respiramos el riesgo a diario.

Cada minuto se combate para evitar ataques y garantizar la seguridad de los activos de las empresas y de los particulares. En el sector de la educación, además, protegemos datos especialmente sensibles: los del alumnado.

No debemos olvidar que existe otro riesgo igual de crítico: el no ser capaces de entender el grado de importancia que tienen las ciberamenazas que nos acechan, porque si no le damos la suficiente relevancia, no conseguiremos tener una protección que esté a la altura de las circunstancias.

Los incidentes en este sector son críticos, —pérdida de matrículas, interrupciones de las clases, caída de las plataformas, sanciones, o pérdidas de reputación— y si no estamos preparados, esas amenazas y otras nuevas seguirán latentes cada día.

Para el CEO de una empresa del sector educativo, la pregunta clave es cómo conseguir una capa de seguridad que asegure la continuidad del servicio educativo al completo, no solo estando preparados para defenderse, sino también cómo poder actuar en caso de que el sistema falle y si esto sucede, se haga con la máxima calidad de respuesta y sin que las finanzas de la empresa se vean comprometidas.

Mi experiencia confirma que este nuevo paradigma exige más espacios de trabajo conjuntos con CEOs, CISOs, CIOs y CFOs para juntos entender las posibles estrategias y posicionar la seguridad como un elemento crucial.

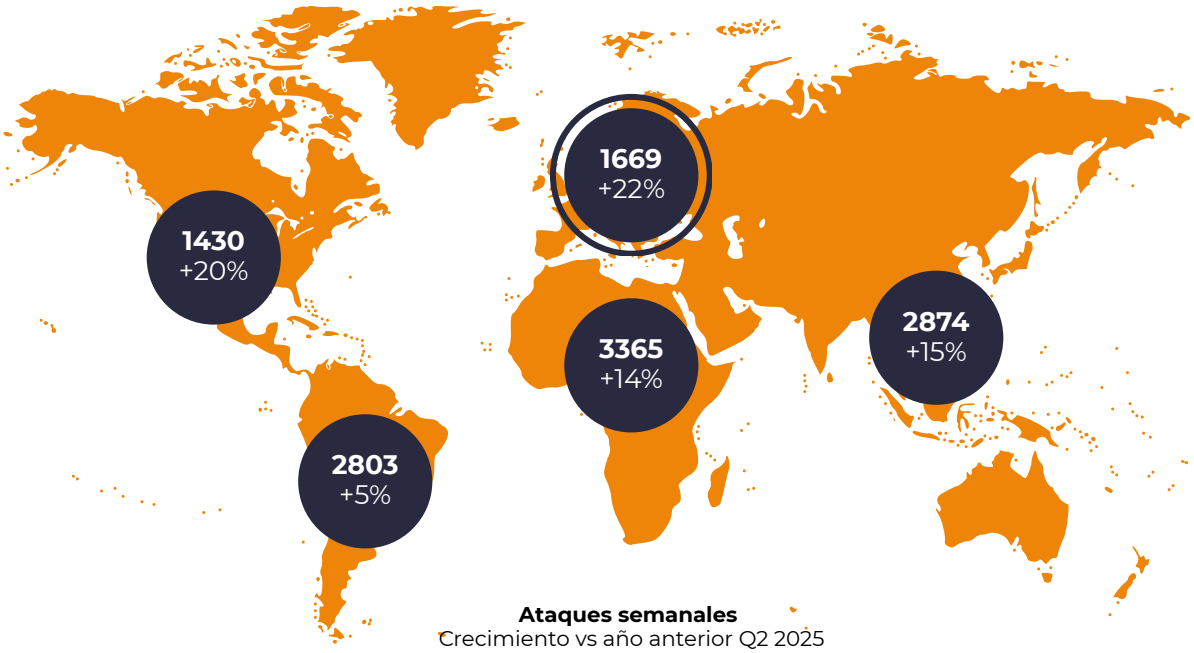
Confío en que este informe anual ayude a ser más conscientes de la realidad en cuanto a la ciberseguridad que existe en el sector educativo.

José Romero
CEO de Sector Asegurador

Índice

01. DATOS **MACRO**

Aunque el volumen medio de ataques semanales en Europa durante el Q2 del 2025 no fue el más alto, se registró el mayor incremento interanual (22%), señal de una tendencia al alza en la actividad de amenazas, impulsada por tensiones geopolíticas, fragmentación regulatoria y una alta concentración de datos valiosos.



Ataques semanales
Crecimiento vs año anterior Q2 2025

Fuente:
Estado de los ciberataques globales - Q2 2025 CheckPoint

Perspectiva Global

A escala global, la ciberseguridad en el sector educativo se centra en la intersección de tres fuerzas: datos extremadamente sensibles (menores, identidad, investigación), infraestructuras cada vez más distribuidas (campus, nube, aprendizaje híbrido, IoT) y asimetrías de recursos frente a adversarios profesionalizados.

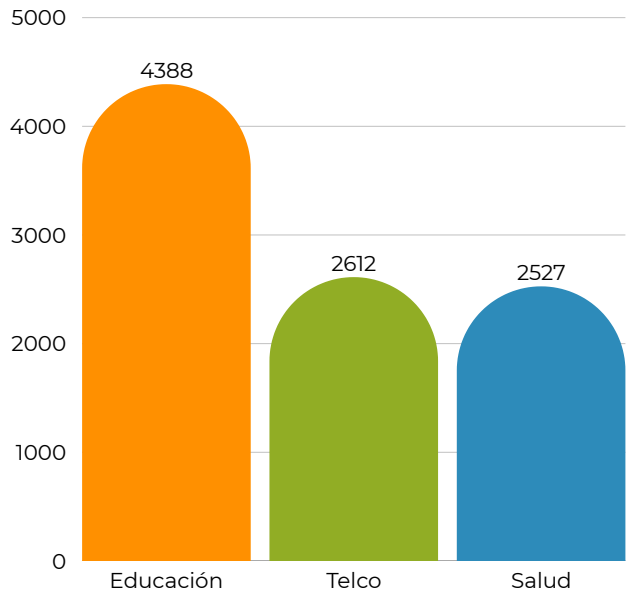
La industrialización del delito —ransomware-as-a-service, kits de phishing personalizados y la explotación automatizada con IA— ha reducido las barreras de entrada y ampliado el alcance de campañas de extorsión y filtración.

A ello hay que sumar los riesgos de la cadena de suministro (proveedores EdTech, integraciones SSO, APIs) y una dependencia crítica de la disponibilidad (exámenes y matriculaciones principalmente), que convierten cualquier interrupción en una crisis operativa y reputacional.

01. ATAQUES AL SECTOR **EN EUROPA**

Se mantiene una presión sostenida sobre el sector educativo, con Europa como la región del mundo donde más crecieron los ataques.

N° de ataques semanales Q2 2025



Estas cifras sitúan al sector educativo como EL MÁS ATACADO de todos los sectores económicos.

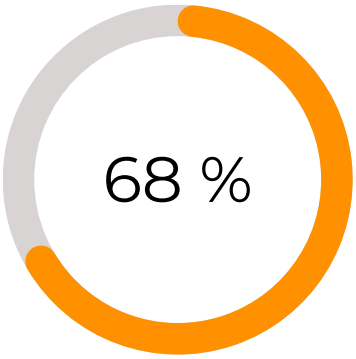
El sector educativo continúa liderando en número de ciberataques en el sector privado (más del doble de la media global) y, además, Europa muestra el mayor crecimiento interanual en volumen regional.

El aumento de ciberataques al sector educativo muestra una presión sostenida, ya que los actores maliciosos apuntan a defensas posiblemente débiles y a intentar acceder a un gran repositorio de credenciales de estudiantes y del profesorado.

Fuente:
Estado de los ciberataques globales - Q2 2025 CheckPoint

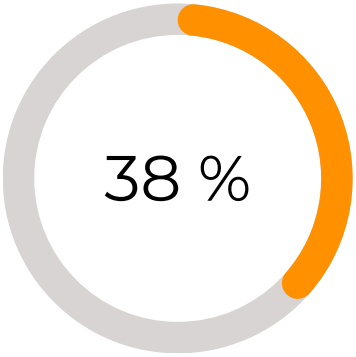
01. LAS ESTADÍSTICAS **EN ESPAÑA**

Cerca de 7 de cada 10 universidades españolas han sufrido ciberataques o ciberincidentes en el último año, según el IMC. Esto refleja una realidad candente, donde es muy difícil escapar a la presión que ejercen los atacantes en los sistemas.



Universidades Atacadas

De las universidades españolas han sufrido ciberataques en el último año.



Incremento Anual

Aumento de ataques respecto al año anterior en el sector educativo.

Cerca de siete de cada diez universidades españolas (67,86%) han sufrido ciberataques o ciberincidentes en el último año: El 32,1% ha sufrido entre dos y cinco ataques anuales y el 17,9% más de cinco incidentes.

Fuente:
Estado de los ciberataques globales - Q2 2025 CheckPoint
Estudio Índice de Madurez en Ciberseguridad (IMC) de MetaRed

02. ¿PORQUÉ **TANTOS ATAQUES**?

Las empresas del sector educativo son un tipo de objetivo estratégico desde el punto de vista del atacante, que centra sus esfuerzos en maximizar el impacto de sus acciones.

Superficie Masiva de Ataque

Miles de estudiantes, docentes y personal administrativo conectados simultáneamente a los sistemas institucionales.

Datos de Alto Valor

Información personal, académica, financiera, investigación e incluso datos sanitarios concentrados.

Sistemas Vulnerables

Infraestructura potencialmente obsoleta y presupuestos limitados para ciberseguridad.

Los ciberdelincuentes consideran las instituciones educativas como **blancos fáciles** con información valiosa.

Fuente:
Encuesta Action 1 a 250 líderes de IT del sector educativo.

Es necesario que nuestra empresa del sector educativo sea capaz de adecuarse al alto grado de exposición al ataque, y sea capaz de priorizar una continuidad operativa y un nivel de gobernanza clara frente a los ciberataques (que incluya un responsable, un marco de trabajo a largo plazo y un nivel de presupuesto acorde), asegurando un nivel alto de protección, capacidad de resiliencia, monitorización 24×7, control de SaaS/proveedores/colaboradores y delegando el riesgo en caso de brecha o ataque efectivo.

Sería interesante completarlo con formaciones prácticas, playbooks de respuesta y cumplimiento RGPD/AEPD, y midiendo el progreso con KPIs ejecutivos.

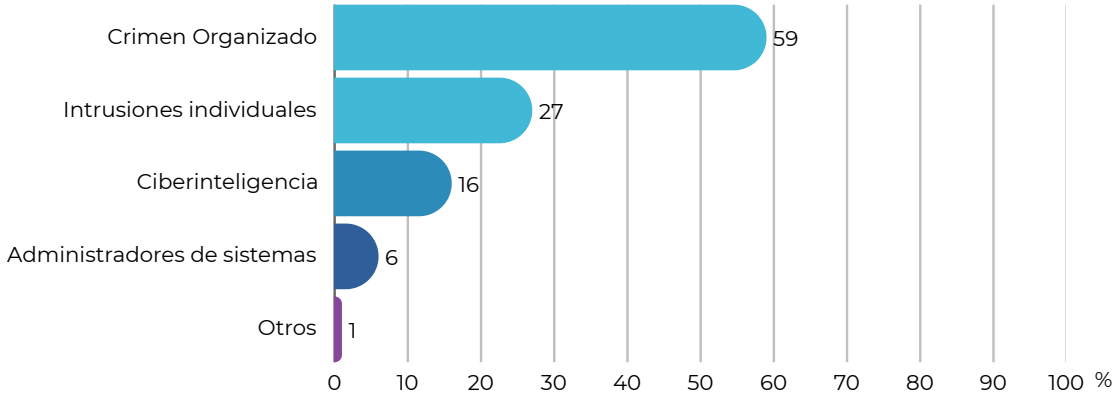
Hay que recordar que el 44 % de las escuelas destina menos del 10 % de su presupuesto de IT a la ciberseguridad, lo que dificulta aún más su capacidad para implementar estrategias de seguridad integrales y que la mayoría de las escuelas (78%) no emplean especialistas en ciberseguridad.

02. ¿QUIÉN HACE ESOS ATAQUES?

Es importante conocer el origen y el tipo más frecuente de atacante para dar prioridad a diferentes estrategias y acciones para mitigar el riesgo de ataque.

% de ataques por origen del atacante

% de ataques por tipo de atacante



Fuente:
Verizon 2025 DBIR Data Breach Investigations Report

Los actores externos están detrás del 62% de los ataques en el vertical de Servicios Educativos, de los cuales, el 59% de ellos corresponde al crimen organizado). Esto tiene sentido si consideramos la prevalencia de ransomware y extorsión en este ámbito.

Los actores internos también representaron una parte significativa de los ataques en la industria de Servicios Educativos, con un 38%. Esto se debe principalmente a personas descuidadas que continúan cometiendo errores de diversa índole.

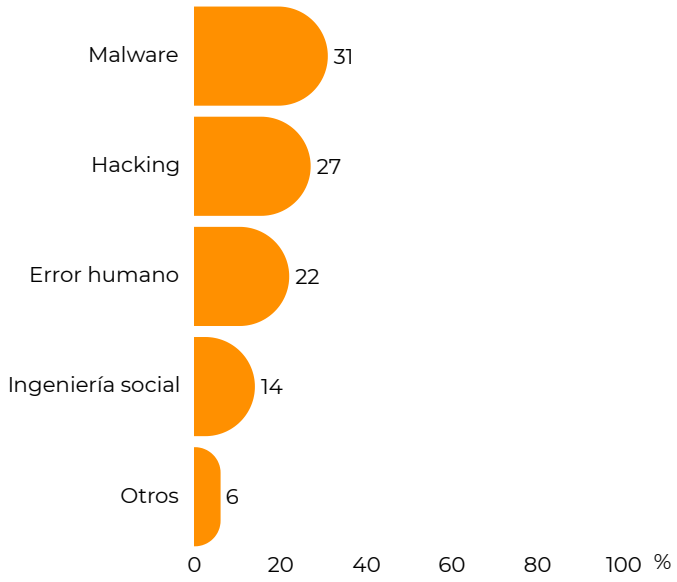
También contribuyen a las cifras internas, aunque en mucha menor medida, los actores internos ocasionales culpables de uso indebido (8%).

Esta situación exige estrategias que combinen defensa frente a amenazas criminales profesionalizadas con la reducción sistemática de errores y abusos internos.

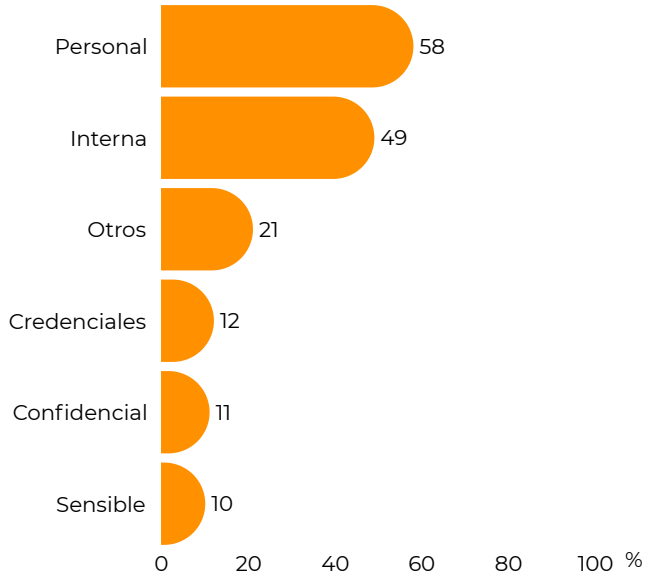
02. ¿QUÉ TIPOS DE ATAQUES Y **QUÉ BUSCAN**?

Al evaluar las acciones que más emplean los actores y conocer qué información buscan, podremos enfocar nuestras estrategias en proteger los principales vectores y los activos más críticos.

% de ataques por tipo de ataque



% de ataques por tipo de ataque



Fuente:
Verizon 2025 DBIR Data Breach Investigations Report

Los patrones de intrusión en los sistemas, el nivel de errores diversos y el uso de ingeniería social se mantienen por tercer año consecutivo, como los tres principales vectores de ataque.

Aunque este año los errores diversos (22%) superaron a la ingeniería social (14%), la intrusión en los sistemas volvió a ocupar el primer lugar.

Esto sugiere que el sector de los servicios educativos está siendo objetivo de actores cada vez más sofisticados, dispuestos a hacer el “trabajo extra” necesario para obtener acceso a los datos de esta industria.

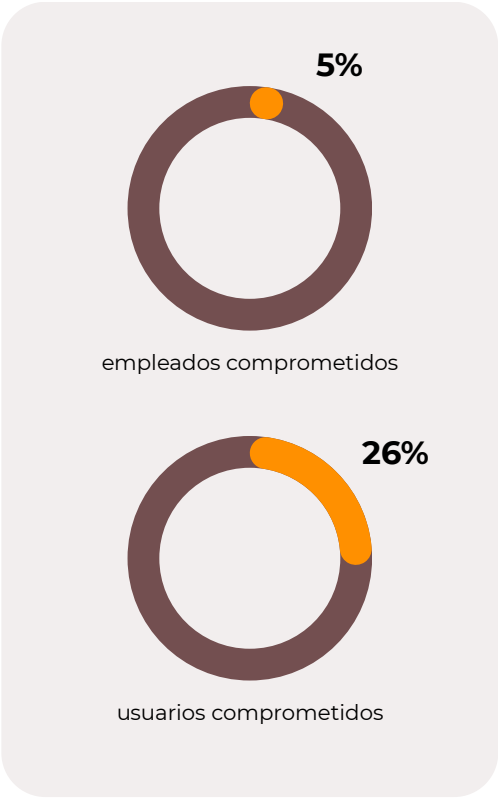
Es necesario añadir que estos ataques suelen ser programados por los ciberdelincuentes, que sincronizan sus campañas con el calendario académico para conseguie el máximo impacto.

02. EL ROBO ES LA **ANTESALA DEL ATAQUE**

El robo de credenciales se ha consolidado como una de las tácticas más comunes y efectivas de los ciberdelincuentes, ya que al obtener nombres de usuario, contraseñas e incluso cookies de sesión legítimos, los atacantes pueden infiltrarse en sistemas críticos sin necesidad de explotar vulnerabilidades técnicas complejas, pasando desapercibidos durante largos periodos de tiempo.

Este tipo de ataque abre la puerta a accesos no autorizados a correos electrónicos, plataformas de gestión académica, servicios en la nube y bases de datos que contienen información sensible de estudiantes, docentes y personal administrativo.

COLEGIOS



Se han analizado 2.270 colegios que disponen de página web propia en España —excluyéndose aquellos cuyo portal pertenece a un servicio público destinado principalmente a las familias— y se ha detectado que en el 26% de estas páginas tienen accesos de sus usuarios (la mayoría de los casos son padres y tutores) a esos portales publicados en la dark web. Esta exposición masiva de credenciales supone un riesgo directo para la privacidad de los menores y para la integridad de los servicios escolares (acceso a notas, comunicaciones y datos financieros), y obliga a los centros a tomar medidas urgentes de mitigación: reposición de credenciales, autenticación reforzada y monitorización de fugas en fuentes ilícitas.

ESTUDIOS SUPERIORES

Se han analizado 216 centros de educación superior y universidades españoles cuyos principales usuarios son los propios alumnos, revelando un panorama especialmente preocupante. El 40% de estas instituciones presenta datos de empleados comprometidos, mientras que el 63% tiene credenciales de estudiantes filtradas, con un total de 141.000 registros de alumnos expuestos en la dark web. Esta situación pone de manifiesto la magnitud del riesgo al que se enfrentan las universidades, donde la combinación de grandes volúmenes de información personal y académica, junto con entornos tecnológicos abiertos y colaborativos, convierte a estas entidades en objetivos prioritarios para los ciberdelincuentes.

Fuente:
Estudio de Sector Asegurador analizando 2700 páginas web de colegios y 216 universidades y centros de estudios superiores en España.
Hudsonrock

03. IMPACTO **ECONÓMICO**

La gravedad del ataque no solo reside en el desembolso que hay que hacer para pagar un rescate o hacer que los sistemas vuelvan a la normalidad, hay otra serie de gastos y pérdidas económicas que hay que tener en cuenta para hacer un balance global de la repercusión en los fondos de la institución educativa.

2,24M€

Coste Medio por Ataque

En el sector educativo, un 48% superior a otros sectores

473K€

Pago de Rescates

Media que las instituciones pagan a los ciberdelincuentes en 2024

230K€

Recuperación Total

Coste adicional para restaurar completamente los sistemas

En el último año, las organizaciones de educación básica han visto cómo el coste medio de recuperarse ante un ataque de ransomware se ha multiplicado por 2,36.

La situación fue aún más crítica en la educación superior, donde los investigadores identificaron un incremento de más de cuatro veces.

Esto refleja una escalada significativa en el impacto financiero de este tipo de ataques dentro del sector educativo.

Un solo ciberataque puede comprometer **décadas de prestigio** institucional, su estabilidad económica y su continuidad académica.

Fuentes:
IBM X Force 2025 Cost of a Data Breach Report
US ransomware monitor - Comparitech
Global threat intelligence from Check Point Research
Cyber security breaches survey 2025 - Gov UK

04. MULTAS GDPR - **GOLPE DOBLE**

Los incidentes de ciberseguridad en el sector educativo no solo implican la pérdida de datos sensibles y la interrupción de la actividad académica, sino que también pueden derivar en importantes multas y sanciones por parte de la Agencia Española de Protección de Datos (AEPD)

20M€

Multa Máxima

O el 4% del volumen de negocio anual por incumplimiento del RGPD

106K€

Multa Media en España

Sanción promedio impuesta por la AEPD en 2024

35,6M€

Total Sanciones 2024

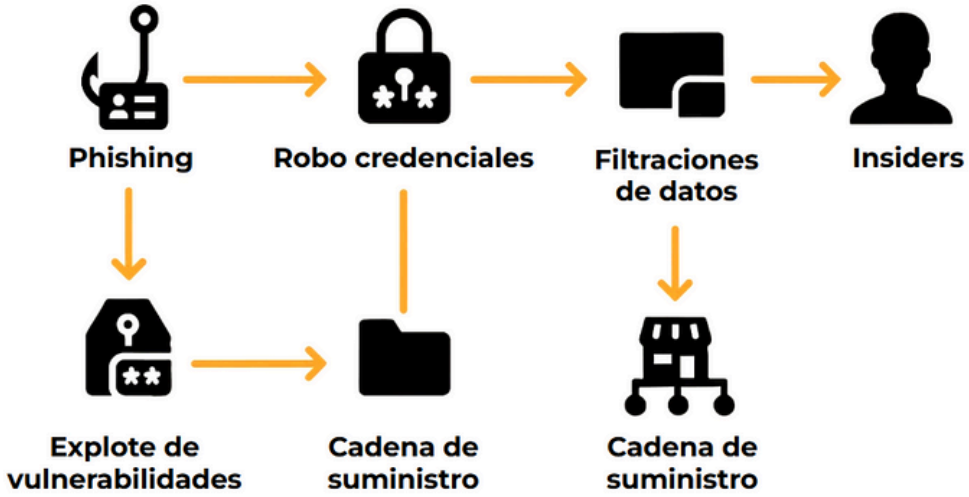
Importe total de multas RGPD impuestas en España el año pasado

La normativa vigente, especialmente el RGPD y la LOPD, exige a las instituciones educativas que garanticen la confidencialidad, integridad y disponibilidad de la información personal que gestionan. Cuando un centro no adopta medidas de seguridad adecuadas o incumple sus obligaciones de notificación ante una brecha, se expone a sanciones económicas significativas, además de un fuerte impacto reputacional que puede afectar a la confianza de estudiantes, familias y personal.

Fuente:
Agencia Española de Protección de Datos (AEPD)

05. VULNERABILIDADES **CRÍTICAS**

La mayoría de los ataques provienen de brechas producidas por phishing, malware y por vulnerabilidades en los sistemas, pero al final todos los eslabones, están conectados.



Phishing e ingeniería social
En un entorno educativo, esto suele implicar un correo electrónico cuidadosamente elaborado que engaña al personal ocupado para que revele sus credenciales de inicio de sesión o se descargue un fichero que acaba en un ataque de malware.

Ransomware
Una vez dentro, el ransomware es la principal forma de cobro para los atacantes. Los atacantes modernos utilizan una táctica de "doble extorsión": primero roban datos y luego cifran los archivos originales, amenazando con filtrar los datos robados si no se paga el rescate.

Vulnerabilidades explotadas
El software sin parchear es una puerta abierta para los atacantes. Este vector de ataque está en crecimiento y ya es responsable del 20 % de las brechas de seguridad. Una brecha de seguridad en un LMS es un claro ejemplo de cómo una sola vulnerabilidad puede explotarse a gran escala. Identificar estas debilidades es un objetivo fundamental de los servicios de pruebas de penetración de aplicaciones web.

Riesgo de proveedores externos
Como muestran los casos de ciberseguridad, las escuelas dependen en gran medida de proveedores externos. Cuando estos proveedores sufren una vulneración de seguridad, los datos de los estudiantes quedan expuestos. La seguridad de una escuela está ahora inextricablemente ligada a la seguridad de su cadena de suministro.

Fuente:
Deepstrike.io
Verizon 2025 DBIR Data Breach Investigations Report

05. CIBERRIESGOS ESPECÍFICOS DEL SECTOR

Es necesario entender que detrás de cada riesgo potencial hay una consecuencia que vuestra institución deberá abordar. Este análisis nos sirve para evaluar si vuestra empresa tiene estas situaciones previstas y bajo control.

1. **Cifren en LMS/ERP/correo**
   Da pie a un parón de facturación, de clases y evaluaciones, especialmente en fechas críticas; con sus respectivos costes de recuperación, asistencia legal, notificaciones, reprogramaciones y asistencia a clientes y proveedores.

2. **Filtren expedientes, datos de alumnos y extorsión**
   Por un robo de credenciales, los atacantes pueden acceder a bases de datos de alumnos y profesores, contratos, facturas, documentación... Con obligación de notificar, defensa jurídica y posibles sanciones y, por otro lado, desembolso económico.

3. **Filtren datos sensibles**
   Riesgo de multas por vulneración de RGPD y reputacional por brechas que afecten a grabaciones e identificaciones con datos sensibles.

4. **Secuestren las cuentas**
   Es la puerta de entrada para que los atacantes envíen phishing o comunicaciones fraudulentas desde cuentas de docentes/dirección, dando como resultado casos de suplantación de identidad, daños a terceros y pérdida de confianza.

5. **Cometan fraude por cambio de IBAN o devoluciones**
   Pudiendo acabar en casos de estafa a clientes con cobros en otra cuenta a través de correos enviados desde la misma empresa (Ej: asunto: “Nuevo número de cuenta”) para cobros de matrículas o pagos a profesores/proveedores, acabando en casos de fraude económico y pérdidas económicas para las partes y demandas judiciales.

6. **Ataques DDoS al campus web en matrícula/exámenes**
   Interrumpiendo el servicio justo cuando más ingresos/actividad hay.

7. **Robo de portátiles/USB sin cifrar**
   Pérdida y filtración de datos de los profesores/alumnos, accesos e información corporativa.

05. LOS FALLOS **SUELEN SER HUMANOS**

El fallo humano sigue siendo el principal vector de entrada para los ciberdelincuentes, especialmente en el sector educativo, donde conviven miles de usuarios con distintos niveles de conciencia digital. Este riesgo se multiplica y convierte la capacitación y la cultura de seguridad en factores críticos.

TIPOS DE ERRORES HUMANOS MÁS COMUNES

- Hacer clic en enlaces o descargar archivos adjuntos maliciosos en correos o páginas diseñadas para robar credenciales o información delicada.
- Usar contraseñas débiles o reutilizadas, facilitando a los atacantes el acceso no autorizado a los atacantes.
- Manejar los datos de manera inadecuada, o negligente, enviando información confidencial al destinatario equivocado, compartir datos públicamente o eliminarlos de forma incorrecta.
- No actualizar el software cuando toca, no instalando parches o actualizaciones, o dejando sistemas expuestos a vulnerabilidades conocidas.
- Haciendo una mala configuración de los sistemas, estableciendo parámetros de seguridad de forma incorrecta, lo que abre la puerta a ataques.

Fuente:
Verizon 2025 DBIR Data Breach Investigations Report

05. RETOS ESPECÍFICOS

Para luchar contra las amenazas y los continuos ataques hay que estar preparados y tener la mayor capacidad de reacción, pero hay una serie de situaciones que pueden lastrar la evolución de nuestro nivel de madurez en ciberseguridad.

Falta de personal

El 40% de las instituciones educativas prevé incorporar nuevo personal en los próximos 12 meses, aunque un 57% reconoce que tiene muchas dificultades para atraer talento debido a los costes salariales y un 55% por la limitada disponibilidad de perfiles especializados.

Falta de procesos

Alrededor del 70% de las instituciones tiene pendiente la creación de procedimientos formales y aprobados para la gestión de incidentes de ransomware.

Sistemas heredados

Las instituciones de educación superior han mantenido equipos que han formado parte de su infraestructura durante décadas.

Los sistemas heredados son difíciles de actualizar y su protección contra los ciberataques modernos supone un reto. Si bien los sistemas actualizados ayudarían a proporcionar una red más segura, la reducción de los presupuestos implica que la financiación puede destinarse a la actualización de sistemas o a medidas de ciberseguridad.

Fuente:
Estudio Índice de Madurez en Ciberseguridad (IMC) de MetaRed

06. CASOS REALES EN ESPAÑA 2025

Cada año se dan casos de ataques que, por el tipo de institución o, por el tipo de ataque, trascienden y nos ayudan a entender hasta dónde pueden llegar las repercusiones.

Escuela de negocios de alto nivel
Según los atacantes del grupo de ransomware Qilin, se habían atribuido la autoría de una brecha de datos en ESIC University (España).
Según el propio grupo, los atacantes habrían exfiltrado 421 GB de información distribuidos en 97.000 archivos, entre los que se incluirían datos personales de más de 66.000 estudiantes y alumni, así como presupuestos, contratos, patrocinios y nóminas del personal.

Empresa top nacional de contenidos educativos
El grupo Hellcat afirmó haber atacado y estar en posesión de archivos sensibles de Santillana, la mayor unidad de negocio del grupo mediático español Prisa, que cotiza en bolsa.

Colegio con más de 150 años de historia
El colegio Compañía de María de Vigo, uno de los colegios más antiguos de la ciudad, también ha sido notificado por parte del grupo de atacantes Arcus Media de haber sido víctima de un ataque de ransomware.

Universidad Balear
Los autores del ataque, del que no se conoce el alcance, enviaron correos electrónicos fraudulentos haciéndose pasar por la institución universitaria. Esos correos incluían una página web falsa que pedía las credenciales institucionales con la intención de obtener información personal.

Fuente:
Ransomware.live
CrónicaBalear

9.7 Millones de alumnos

La cantidad de datos de alumnos que pueden ser expuestos en España.

06. OTROS CASOS INTERNACIONALES

En otros países del mundo se han dado casos mediáticos, especialmente por el volumen de datos de alumnos que se han visto comprometidos.

Universidad de investigación de primer nivel

Según los datos de la propia universidad, el atacante tuvo acceso no autorizado durante semanas, comprometiendo datos de 870.000 usuarios afectados. Según la notificación de la propia universidad, los datos filtrados incluían nombres, fecha de nacimiento y número del seguro social, datos de contacto, información demográfica, historial académico, información financiera y cualquier información relacionada con seguros e información médica que el usuario haya proporcionado.

Escuela digital internacional

Un estudiante universitario de 19 años, se declaró culpable de los cargos federales por liderar un ciberataque masivo contra PowerSchool, una plataforma educativa ampliamente utilizada en Estados Unidos y Canadá. Tuvo acceso a datos sensibles de 60 millones de alumnos y docentes, datos con notas y contactos.

Universidad local con 150 años de historia

El grupo Meow realizó un ataque de ransomware y bloqueando sus sistemas, acto que impidió que la entidad pudiera realizar las matrículas, afectando directamente a la recaudación de fondos. Se vieron obligados a cerrar tras el ciberataque. Los atacantes pusieron a la venta 21 GB de datos confidenciales por un valor de 25K$. Es el segundo ataque que recibía la entidad.

Estos incidentes reales convierten las amenazas abstractas en riesgos tangibles. Estas recientes brechas de alto nivel ponen de manifiesto una cadena de fallos sistémica e interconectada en el ecosistema de la ciberseguridad en el sector educativo.

Fuente:
Ransomware.live

07. SE NECESITA PROTECCIÓN INTEGRAL

Para evitar todos estos riesgos y tipologías de ataque, necesitamos abordar una serie de puntos para conseguir un nivel de protección preventiva y proactiva de forma global.

- Protección en todos los dispositivos corporativos, controlando sus privilegios, sus acciones y realizando un mantenimiento adecuado.
- Registro y monitorización (personal que controla la ciberseguridad de la empresa y sistema de alertas de comportamientos anómalos).
- Accesos con múltiple factor en los elementos críticos, como los servidores, la plataforma de formación, las aplicaciones móviles, CRM, ERP y donde se usen contraseñas, que sean únicas y cambiadas con cierta frecuencia.
- Doble comprobación con clave de seguridad en pagos importantes que se realicen entre administración y dirección.
- Procesos para gestión de accesos (altas/bajas automáticas del personal contratado, docentes y alumnos por curso/convocatoria).
- Cifrado obligatorio en el servidor, ordenadores y medios extraíbles.
- Backups probados y plan de continuidad (“¿qué hacemos si el LMS cae hoy?”).
- Segmentación de las redes (alumnos/invitados vs. administración/finanzas).
- Protección web: WAF y medidas anti-DDoS para portal de matrícula y campus.
- Formación anti-phishing al personal docente/administrativo y simulacros periódicos.
- Due diligence de proveedores (SaaS del campus, videoconferencia, pago): SLA, seguridad, backups y soporte en incidentes.
- Política de control de la propiedad intelectual y revisión de materiales docentes.

Métricas vinculadas al sistema de protección

Formar y concienciar al personal de la empresa

Controlar los recursos más críticos

07. PIRÁMIDE **ANTI-CIBERRIESGOS**

La ciberprotección en el sector educativo debe construirse desde una visión integral que priorice los riesgos y abarque todo el espectro de los posibles de vectores de ataque de forma eficaz.

Al igual que estamos preparados ante un incendio o un robo, e incluso hacemos simulaciones, tenemos que seguir la misma estrategia cuando hablamos de ciberseguridad.

Implementar estas medidas minimiza la exposición al riesgo y hace que los atacantes lo tengan más difícil para penetrar en los sistemas, lleguen a suplantar la identidad de algún miembro y se es capaz de detectar comportamientos anómalos con la máxima agilidad.

Para ello, es fundamental destinar los recursos técnicos y de personal para garantizar un nivel de protección que sea capaz de detener las olas de amenazas frecuentes y cada vez más especializadas.

07. SISTEMA DE CERO CONFIANZA

El modelo “Zero Trust” parte de la idea de que ningún usuario o dispositivo es de confianza por defecto, ni siquiera estando dentro de la red interna. En el sector educativo, su adopción es clave para reducir la superficie de ataque y proteger los datos sensibles frente a accesos no autorizados.

Monitorización continua
Evaluando cada intento de acceso como si fuera un evento potencialmente peligroso.

Accesos con el mínimo nivel de privilegios
garantizando que los usuarios solo disponen de los permisos estrictamente necesarios.

Suponer que siempre hay un alto nivel de riesgo
actuando siempre bajo la premisa de que la red podría estar comprometida en cualquier momento.

En ciberseguridad, los ciberdelincuentes suelen entrar de forma sigilosa, sin hacer mucho ruido, intentando pasar desapercibidos.

Es necesario recalcar que en el 77% de los incidentes de ransomware, los ataques maliciosos se hicieron dentro de los 30 días posteriores a una interacción inicial, y el 54% dentro de los primeros siete días.

De ahí la importancia de adoptar un sistema “Zero Trust”, donde desconfiar es algo estrictamente necesario.

La preparación, la priorización y la capacidad para mitigar futuros ataques son esenciales para tener un nivel de protección a la altura de las circunstancias.

Fuente:
Estrategias de protección y contención contra ransomware - Mandiant

08. HAY NUEVAS AMENAZAS - **IA**

Actualmente, 1 de cada 6 ataques a nivel global son hechos por IA. El año pasado, el sector educativo estuvo analizando y debatiendo sobre el uso de la IA en el sector educativo, viendo las posibilidades, retos y amenazas que esta nueva tecnología iba a suponer para el sector.

Los ciberatacantes utilizan cada vez más herramientas de IA para crear correos electrónicos de phishing convincentes que roban datos confidenciales y falsifican identidades, pudiendo suplantar la identidad digital de la institución o creando avatares falsos de educadores o del personal directivo para engañar las víctimas.

Phishing 2.0

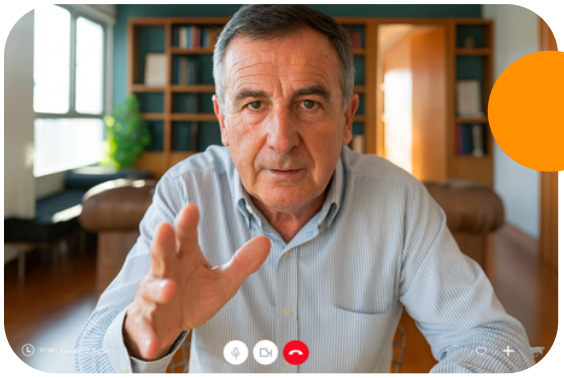
La IA permite generar correos electrónicos y mensajes con un lenguaje natural impecable, personalizados en función del perfil de la víctima y sin los errores ortográficos o gramaticales que antes delataban un fraude. Esto incrementa de forma notable la tasa de éxito de los ataques, ya que los mensajes resultan más convincentes y difíciles de distinguir de una comunicación legítima.

Vishing (phishing por voz)

Los modelos de clonación de voz basados en IA permiten suplantar con gran realismo a directivos, profesores o personal administrativo. De este modo, los atacantes pueden inducir a empleados o estudiantes a revelar información sensible o autorizar transferencias, confiando en la voz de una figura reconocida.

Deepfakes de audio y video

Representan una amenaza en rápido crecimiento para las instituciones educativas. Estas falsificaciones hiperrealistas pueden usarse para difundir desinformación, manipular a la opinión pública, dañar la reputación de un centro o incluso extorsionar a directivos y estudiantes. La combinación de accesibilidad tecnológica, bajo coste de producción y un realismo sin parangón, convierte a esta técnica en un riesgo tangible, que obliga a reforzar la verificación de identidades, la concienciación del personal y los sistemas de doble verificación.



Además, los actores maliciosos pueden manipular chatbots y herramientas digitales basadas en IA para distribuir malware o recopilar información de los usuarios, lo que supone riesgos significativos para el sector educativo

Fuente:
ENISA Threat Landscape 2024
IBM X Force 2025 Cost of a Data Breach Report

08. Y EL USO DE **LA IA SE MULTIPLICA**

Hay una amenaza emergente muy cercana y que está vinculada con el riesgo de fuga de información corporativa sensible por el uso indiscriminado de las plataformas de GenAI. Un 15% de los empleados accede de forma rutinaria a estos sistemas desde dispositivos corporativos (al menos una vez cada 15 días).

Lo más preocupante aún es que gran parte de esos accesos se realizaba empleando correos electrónicos personales como identificador de la cuenta (en un 72% de los casos), o bien correos corporativos sin sistemas de autenticación integrados (17%), lo que sugiere un uso fuera de las políticas de seguridad establecidas.

Fuente:
Verizon 2025 DBIR Data Breach Investigations Report

08. ATAQUES AUTOMÁTICOS A ESCALA CON IA

El año pasado, el sector estuvo analizando y debatiendo sobre el uso de la IA en el sector educativo, viendo las posibilidades, retos y amenazas que esta nueva tecnología va a suponer para el sector.

Los ciberatacantes modernos utilizan todo el potencial de los nuevos modelos de IA especialmente capaces en tareas relacionadas con la programación y análisis de código.

Mutaciones de Malware
Los hackers son capaces de crear cientos de variaciones de un mismo virus y simulando ser un fichero convencional, son capaces de hacer que estos pasen desapercibidos.

Detección de Brechas
La inteligencia artificial es capaz de evaluar código, detectar posibles vulnerabilidades de forma automática y realizar ataques sin apenas intervención humana.

Fuente:
ENISA Threat Landscape 2024

09. Y TENER BUENA COBERTURA **IMPORTA**

Contar con un ciberseguro no solo es delegar el riesgo, es contar con una protección que va más allá de tener asistencia en el momento del ataque, tanto a nivel de respuesta como a nivel legal. Es proteger la economía de la empresa frente a este tipo de imprevistos que pueden lastrar todo el trabajo del año.

Nuevas soluciones preventivas

La propia póliza puede incluir una solución que te ayuda a prevenir y monitorizar tus activos digitales e incluso delegar parte de la protección.

Respuesta Inmediata

Equipo especializado disponible 24/7 para contener y neutralizar amenazas en tiempo real, suponiendo un menor gasto para la aseguradora.

Soporte legal

Además de la respuesta técnica, es preciso gestionar la crisis reputacional, y la comunicación con la AEDP para evitar multas y sanciones.

Recuperación Completa

Soporte en la restauración de datos y en poder recuperar el control de los sistemas lo antes posible y así poder volver a la normalidad.

Fuente:
Sector Asegurador - Análisis de condicionados generales 2025

¿Y qué cubren?

El ciberseguro es un paquete de coberturas integral, que da protección ante los principales eventos que puedan suceder y que afecten de forma directa a la economía y reputación de la empresa.

- **Pago de extorsión**
- **Pérdida de beneficios**
- **Daños propios**
- **Daños a terceros**
- **Fraude**

09. EL ROI DEL **CIBERSEGURO**

El ciberseguro se ha convertido en un aliado estratégico para las instituciones educativas, que a menudo operan con presupuestos ajustados y una alta exposición a ciberamenazas.

Protección
Devastación **VS**

Una póliza de ciberseguridad no es un gasto, **es la inversión más rentable** para tu institución.

2,24M €

Ataque medio, incluyendo posibles rescates, pérdida de beneficios, multas o sanciones, pero sin contar el valor de la pérdida reputacional.

▲ 1-15K€ año

Coste promedio de una póliza cuyo precio dependerá de la facturación de la empresa, volumen de usuarios, siniestralidad y grado de protección.

▲ ROI: 16.500

La rentabilidad promedio de la contratación de un seguro que te ofrece no solo protección en caso de sufrir un ataque, también te ayuda a aminorar el riesgo, minimizando las pérdidas.

Frente a incidentes de ransomware, filtraciones de datos de estudiantes o personal, e interrupciones críticas de servicios académicos, una póliza adecuada ofrece un respaldo financiero para cubrir un servicio efectivo de respuesta, reduciendo el tiempo de vuelta a la normalidad.

Además, proporciona acceso a equipos de forenses especializados, mediación y comunicación de crisis, recursos que muchos centros no podrían sostener por sí mismos de forma permanente sin este tipo de protección.

Fuente:
Sector Asegurador - Análisis tarificaciones ciberseguros 2025

09. PREGUNTAS QUE HACERSE

Muchas veces no somos conscientes de lo importante que es tener protección hasta que la necesitamos, pero en esos momentos ya puede ser tarde.

DINERO

¿Cuánto os costaría tener la empresa parada sin que nadie pueda acceder a las plataformas o a los sistemas?

SERVICIO

¿Cuánto te costaría el que alguien te ayude a saber qué está pasando y que además te ayude a salir de la situación donde estás?

TIEMPO

¿Cuánto tiempo crees que tardarías en resolver la brecha y abordar todos los asuntos relacionados?

MULTAS

¿Qué pasará si te multan por si tus prácticas de seguridad no han podido cumplir con las políticas y requisitos de seguridad?

Las organizaciones educativas no pueden permitirse ignorar las consecuencias reales de un incidente de ciberseguridad: las pérdidas económicas, la paralización del servicio, intentar evitar las sanciones de la AEPD por incumplimiento normativo, , los costes externos para recibir apoyo especializado y, lo más valioso, el tiempo perdido en recuperar la normalidad. Cada uno de estos factores impacta directamente en la sostenibilidad del negocio y en la confianza de clientes, estudiantes o empleados.

09. ¿CÓMO SÉ SI **NECESITO UN SEGURO**?

Si diriges o formas parte de la administración de una empresa del sector educativo, es necesario que consideres un ciberataque como un riesgo crítico para vuestro negocio. Estos puntos están orientados a situar nuestra empresa de ecuación y ver hasta qué punto necesitáis un ciberseguro. Cumpliendo uno o varios de ellos, sería recomendable la contratación de un seguro que os proteja ante ciberataques.

- **Facturación > 50.000 € anuales**: Si se produce un ciberincidente en el gestor de matrículas o en la plataforma de clases online o en la de facturación, va a impactar directamente en los ingresos y en la reputación de la empresa.
- **Trabajáis con clientes corporativos**: En caso de que os ataquen a vosotros, pueden atacar a las empresas con las que trabajáis, siendo parte de un ataque llamado cadena de suministro. Os expone a reclamaciones por daños y perjuicios, pérdida de clientes importantes y pérdida de reputación.
- **Cobráis matrículas/pagos online (TPV, pasarela, SEPA)**: Si se comprometen los datos de pago o si hay un fraude, te expones a devoluciones, reclamaciones y puede acabar en denuncias.
- **Dependéis de un LMS/ERP/campus virtual:** (Moodle, Aula1, SDI, Odoo, etc...) Si se cae, u os atacan, se paralizan la facturación, las clases, las evaluaciones, los certificados... Además, a los usuarios les pueden robar las credenciales e intentar atacar la plataforma desde dentro.
- **Gestionáis >25 alumnos/proveedores o varios grupos/convocatorias**: No es solo tu daño: si afecta a terceros, pueden reclamaros.
- **Tratáis datos personales sensibles**: Expedientes, notas, becas, DNIs, necesidades educativas, datos de menores, accesos biométricos o incluso grabaciones de clases. Os exponéis a tener multas de la AEDP.
- **Docencia híbrida y cuentas sociales activas**: Si os secuestran los perfiles o los accesos a las plataformas, puede haber un daño reputacional y a terceros si publican cosas en vuestro nombre.
- **BYOD (Bring Your Own Device) y alta rotación de docentes/colaboradores:** Más superficie de ataque y una mayor probabilidad de errores humanos que son la principal puerta de entrada a los atacantes.
- **Misma red Wi-Fi para alumnos y visitantes:** Si no está segmentada, puede ser otra puerta de entrada a la red administrativa.

10. ES NECESARIO **SER MÁS RESILIENTE**

A partir de aquí es cuestión de activar mecanismos dentro de la empresa que hagan que esta sea más resiliente y esté adaptada al nuevo paradigma de ciberseguridad.

RAZÓN 01.

Tendencia Exponencial

Los ataques al sector educativo aumentaron un 38% en 2024, superando el crecimiento de cualquier otro sector

RAZÓN 02.

Rescates Multiplicados

El coste del rescate se multiplicó por 7: de 199.000€ a 1,5 millones€ en solo un año

RAZÓN 03.

No es "Si", es "Cuándo"

El 67,86% de universidades son atacadas, cada día que pasa sin la protección adecuada aumenta exponencialmente el riesgo

RAZÓN 04.

La IA como amenaza

Por que la IA no descansa y hace el trabajo sucio, acortando los tiempos entre la brecha y el ataque.

La ciberseguridad debe asumirse como una inversión estratégica y transversal, integrada en la cultura corporativa y apoyada por la dirección. Establecer políticas claras, reforzar la protección de los sistemas y datos críticos, desplegar tecnologías de detección y respuesta y, sobre todo, concienciar al factor humano permitirá reducir el riesgo de exposición.

El momento de actuar es ahora: implementar un plan de ciberprotección sólido no solo fortalece la resiliencia frente a ataques, sino que posiciona a la organización como referente responsable y confiable en su sector.

10. CONCLUSIÓN

El sector educativo español enfrenta la mayor crisis de ciberseguridad de su historia. Con ataques que cuestan hasta 2,34 millones de euros y multas que pueden alcanzar los 20 millones, la protección ya no es opcional.

1. La educación es la industria más atacada a nivel mundial en 2025.
2. Las escuelas promediaron 4.388 ciberataques por semana → +38 % interanual.
3. Phishing personalizado + ransomware que explotan sistemas sin parches.
4. Altos costes de recuperación + importante interrupción del negocio.
5. Carencia de seguro: Solo el 30% de los negocios disponen de esta cobertura.

Protege el futuro de tu institución

> "La póliza de ciberseguridad es la inversión más rentable que una institución educativa puede hacer para proteger su futuro, su reputación y su continuidad operativa."

¿Y ahora qué?

Revisar el nivel de las defensas: Protección perimetral, de endpoints, MFA, parches al día, copias de seguridad, capacitación del personal, planes de respuesta...

Seguridad proactiva = auditorías + plataformas de pruebas continuas para descubrir riesgos ocultos

Disponer de una póliza de ciberriesgos que mitigue las pérdidas económicas derivadas de un ataque con éxito.

ES MOMENTO DE ESTAR A LA ALTURA

GRACIAS

SECTOR
ASEGURADOR

www.sectoraseguradador.es
comercial@sectoraseguradador.es
(+34) 91 00 545 00