Publicado en México el 16/02/2022

# [La seguridad en línea debe seguir siendo fundamental en la educación según DigiCert](http://www.notasdeprensa.es)

## Las instituciones educativas deben brindar a sus usuarios (estudiantes, docentes, administradores) las herramientas informáticas necesarias para proteger sus computadoras, tabletas y teléfonos, así como para proteger la información de la institución educativa

 La seguridad de los niños y adolescentes cuando navegan por Internet o participan en las redes sociales es una preocupación constante y justificada tanto para los padres como para la sociedad en su conjunto. En cuanto a la educación, si bien son varias las instituciones que regresan a las clases presenciales, la ciberseguridad sigue siendo un factor fundamental, sobre todo para los estudiantes que continuarán su educación a distancia. Tanto en los hogares como en las instituciones educativas, se deben tomar acciones para que los estudiantes adopten comportamientos responsables y preventivos que los mantengan alejados de potenciales ciberamenazas. Ciberamenazas latentesAntes de la aparición de la pandemia, se hizo evidente que en muchos casos, tanto las escuelas como los docentes no estaban lo suficientemente preparados para enfrentar los ataques cibernéticos y lograr mantener la seguridad de los programas y los estudiantes. Factores como la autenticación, el control de acceso, la integridad de los datos y la protección del contenido fueron fundamentales en este problema. Sin duda, el ransomware fue y sigue siendo una de las principales amenazas en los entornos educativos, ya que la escala y el impacto de este delito fue importante en el sector educativo en todo el mundo. Este problema confirma la vulnerabilidad de la industria y la grave amenaza cibernética que representa el ransomware, que incluye organizaciones como escuelas, universidades e instalaciones de investigación. Por ejemplo, en 2020, en el caso de Estados Unidos, más de 500 escuelas y universidades se vieron afectadas por ransomware y los hackers extorsionaron $1,6 millones. Países como Colombia, México y Brasil han experimentado la mayor cantidad de ataques en América Latina en 2021. Ante este escenario, para garantizar el aprendizaje en línea, los sistemas educativos deben resolver dos grandes desafíos: primero, deben proteger sus datos confidenciales, y luego deben proteger sus clases y comunicaciones en línea. Siempre es mejor prevenirEs importante comenzar siempre por asegurar los datos de los estudiantes considerando que las escuelas tienen grandes cantidades de información; Además de los puntajes de las pruebas y las calificaciones, también recopilan la edad, la raza, el género, las necesidades de educación especial, la asistencia, el comportamiento y más sobre sus estudiantes. Estos datos deben estar encriptados y tener restricciones de acceso donde sea que estén alojados. Es fundamental recordar que los sitios de las instituciones educativas deben esforzarse en que sus sitios web sean lo más seguros posible, es por ello que el sitio web de la organización debe estar protegido con un certificado TLS/SSL para encriptar la información y garantizar la confianza en su sitio. Hay tres tipos de certificados TLS: Validación de dominio (DV), Validación de organización (OV) y Validación extendida (EV). “Las autoridades de certificación (CA), como DigiCert, validan cada tipo de certificado con un nivel diferente de confianza del usuario. Los certificados EV brindan el más alto nivel de autenticación y son el estándar global para cifrar datos altamente confidenciales”, afirma Dean Coclin - director senior de desarrollo empresarial de DigiCert. Otra forma en que las escuelas han agregado una capa de seguridad a su aprendizaje en línea es entregando dispositivos a los estudiantes, que deben usarse para acceder a sus trabajos de clase y enlaces de videoconferencia. Sin embargo, esto también requiere administrar dispositivos de forma remota. Puede hacerlo a través de la Administración de dispositivos móviles (MDM). PKI puede resolver la parte de identidad y acceso de la gestión de MDM. MDM puede brindarle control sobre los dispositivos y el perfil de seguridad y el nivel de acceso para los usuarios de dispositivos. “En el caso del correo electrónico, los estudiantes están sujetos al mismo tipo de ataques de phishing que los empleados corporativos. Aunque no hay necesariamente una ganancia financiera, los piratas informáticos lo hacen por varias razones y luego bloquean a los estudiantes reales” agrega Dean Coclin . Especialmente con los dispositivos proporcionados por la escuela, es clave asegurarse de que los estudiantes no instalen accidentalmente malware en la propiedad de la escuela. Puede asegurar el correo electrónico a través de protocolos como S/MIME y trabajar para obtener la certificación DMARC para su dominio. Esta solución evita que los piratas informáticos se hagan pasar por profesores o administradores del dominio de correo electrónico de la escuela. Finalmente, si las instituciones no quieren que los estudiantes manipulen sus boletas de calificaciones o diplomas, es fundamental proteger los documentos confidenciales con la firma digital de documentos. La firma digital de documentos permite a las personas y organizaciones agregar una firma digital a un documento para probar la identidad y la autenticidad del remitente. , este método es más seguro que las firmas escaneadas o los boletos electrónicos, que pueden manipularse fácilmente. Además, nunca caduca y sigue las normas locales, por lo que los documentos pueden ser legalmente vinculantes. Principales retos de la ciberseguridad en la educación durante 2022Entre los principales desafíos se encuentra la continuidad de un número considerable de estudiantes (e incluso docentes), quienes seguirán trabajando en forma remota debido a las posibles variantes del covid-19. Dado que la mayoría de los estudiantes se encuentran fuera de los límites tradicionales establecidos por el departamento de TI, las instituciones educativas deben proporcionar a sus usuarios (estudiantes, docentes, administradores) las herramientas de TI necesarias para proteger sus computadoras, tabletas y teléfonos, así como para proteger la información del institución educativa. Por lo tanto, es necesario proporcionar un software antivirus que pueda ejecutarse en dispositivos Windows, Mac, iPhone y Android. Asimismo, exigir una autenticación fuerte, como la autenticación de dos factores con certificados digitales, que da confianza al departamento de TI, ya que el usuario es quien dice ser. Además, el departamento de TI de la educación necesita reforzar su defensa cibernética, no sólo con firewalls, sino también con herramientas avanzadas de detección de intrusos, para garantizar que los ciberdelincuentes no entren y planten herramientas nefastas que luego puedan usar para exfiltrar datos. Estos datos contienen información de identificación personal sobre los estudiantes que se puede utilizar para hacerse pasar por usuarios ante entidades como bancos y agencias gubernamentales.

**Datos de contacto:**

Prensa DigiCert Latam

573125893314

Nota de prensa publicada en: [https://www.mexicopress.com.mx/la-seguridad-en-linea-debe-seguir-siendo\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Software Ciberseguridad



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)