Aprendizaje en línea seguro

Guía escolar para la protección de datos de los estudiantes en América Latina

eon resilience lab by C Minds

BID

Aprendizaje en línea seguro

Guía escolar para la protección de datos de los estudiantes en América Latina

Autoras: **Claudia May Del Pozo**, **Ana Victoria Martín del Campo Alcocer** y **Mariana Róo Rubí** (Eon Resilience Lab, C Minds).

Contribuidoras: **Constanza Gómez Mont** y **Daniela Rojas Arroyo** (C Minds); **Cristina Pombo** y **Natalia González Alarcón** (BID Sector Social); **Elena Arias** (BID Sector Educación).

https://www.iadb.org/

Tabla de contenido

Agradecimientos

Por todas sus contribuciones, en especial sus aportes de conocimientos que ayudaron a fortalecer la investigación, agradecemos a las personas integrantes de nuestro Consejo Asesor:

Ana Cecilia Pérez Rosales, Co-Fundadora y Co-Directora, CAPA 8, Escuelas Ciberseguras (México); **Carla Vázquez Wallach**, Especialista en derecho digital y fundadora de Legal + Innovation (México); **Cristina Martínez Pinto**, Fundadora y Directora del PIT Policy Lab (México); **Lucía Acurio**, Fundadora y directora de Escuelas Digitales (Perú); **Priscila Gonsales**, Directora nacional de Educadigital (Brasil), y **Santiago Paz**, Especialista Sectorial en Ciberseguridad del Banco Interamericano de Desarrollo (BID) (regional).

Asimismo, expresamos nuestro reconocimiento a las personas entrevistadas durante la investigación, pues sus perspectivas fueron claves para enriquecer el documento:

Andrew Young, Director de conocimiento de The Gov Lab (Estados Unidos); **Alejandro Morduchowicz**, Especialista Líder en Educación en la División Educación del BID (regional); **Cecilia Hughes**, Jefa de Evaluación y Monitoreo del Plan Ceibal (Uruguay); **Diego Russo**, Analista de Ciberseguridad del Plan Ceibal (Uruguay); **Fernando Valenzuela**, Fundador de Global EdTech Impact Alliance (global); **Gabriela Castro**, Directora del Departamento de Recursos Tecnológicos, Gobierno de Costa Rica (Costa Rica); **Leda Muñoz**, Directora de la Fundación Omar Dengo (Costa Rica); **Lindsey Barret**, Investigadora de la Universidad de Georgetown, Fondo de las Naciones Unidas para la Infancia (UNICEF) (Estados Unidos); **Lucía Acurio**, Presidente ejecutiva de Educatec (Perú); **Marcelo Cabrol**, Gerente del Sector Social del BID (regional); **Marcelo Pérez**, Especialista Líder en Educación en la División Educación del BID (regional); **Miguel Brechner**, Especialista Líder en Educación en la División Educación del BID (regional); **Monserrat Creamer**, Especialista de Educación (Ecuador); **Priscila Gonsales**, Directora Nacional de Educadigital (Brasil), y **Víctor Giorgi**, Director General del Instituto Interamericano del Niño, la Niña y Adolescentes del Organismo de los Estados Americanos (OEA) (regional).

Por su registro o participación en el conversatorio regional y sus importantes puntos de vista, le damos las gracias a estos docentes:

Carola Betzabé Huaringa Ospino (Perú), **Enrique Castañeda Zuñiga** (Perú), **Gabriela Pagliaso** (Argentina), **Graciela Pozzer** (Argentina), **Gloria Elizabeth Galeano Álvarez** (Paraguay), **Iris Peña** (Panamá), **Patricia Santanaria Guaminí** (Ecuador), **Roberto Antonio Carmona Caro** (Colombia) y **Silvia Medina** (Argentina).

Además, un agradecimiento a **Juan Pablo Carsi Reyna** (México), Co-fundador y Co-Director de Capa 8, por fungir como revisor del documento. Por último, un especial agradecimiento a nuestros socios de difusión de la Encuesta regional, por sumarse con tanto entusiasmo a la propuesta:

Enseña por México (México), **Fundación Lewis Galindo** (Panamá), **Fundación Omar Dengo** (Costa Rica), **Fundación Quirós Tanzi** (Costa Rica) y **Profesoras Conversando** (Perú).

I. Introducción y contexto

1. Introducción

Las instituciones escolares, tradicionalmente, han sido el segundo hogar de los estudiantes, pero a raíz de la pandemia del COVID-19 se volvieron un espacio únicamente virtual. En él, tanto físico como virtual, se procura su bienestar fisiológico, educativo y emocional, teniendo en el centro un aspecto elemental: su seguridad. La protección integral de los estudiantes incluye los aspectos físico y mental, así como la protección de su información, tarea que hoy en día se debe extender al mundo digital.

En los últimos diez años (Arias Ortiz y Cristia, 2014), en las instituciones escolares se han visto avances significativos en la incorporación de tecnologías disruptivas en las aulas. Esta tendencia se aceleró (UNICEF, 2019) frente a la situación crítica que atraviesan Latinoamérica y el mundo: la pandemia del COVID-19, la cual representó un reto para escuelas y colegios que, en cuestión de semanas y a modo de emergencia, tuvieron que migrar a plataformas digitales para mantener cierta continuidad en los procesos de enseñanza y aprendizaje. Como consecuencia de la actividad en línea, han surgido grandes cantidades de datos digitales de estudiantes y docentes que ahora están en la nube (ONU, 2020). Actualmente, los estudiantes tienen datos en páginas web de compañías, registros en plataformas de administración para gestión educativa y cuentas en servicios de transmisión de audio y video[1].

Si bien las instituciones escolares han asegurado con éxito la protección de los datos físicos de sus estudiantes, en este momento se les presenta un nuevo reto: la protección de su identidad digital y su huella de datos en plataformas educativas digitales. Según la Encuesta Aprendizaje en línea seguro LATAM realizada en siete países de la región[2] por el Banco Interamericano de Desarrollo (BID) y el Laboratorio de Resiliencia Eón de C Minds para fines de esta Guía, se encontró que 16,7% de los docentes no es consciente de los riesgos que puede implicar tener datos digitales de sus estudiantes en las redes, y 43% de los docentes no sabe si ha ocurrido un ataque de ciberseguridad o una fuga de datos en su escuela.

Esta misma encuesta reveló que únicamente 19,5% de las instituciones educativas solicita autorización escrita o digital de los padres de familia de los estudiantes para usar plataformas y herramientas digitales. Además, según esta misma encuesta, 53,12% de los docentes no lee las políticas de privacidad al momento de empezar a usar este tipo de plataformas, lo que implica que no conoce cómo los datos de sus estudiantes (y los suyos) están siendo utilizados.

1 De acuerdo con la ONU, la computación en la nube entraña el uso de recursos informáticos y de TIC que se proporcionan como un servicio a través de Internet desde ubicaciones geográficamente diversas, utilizando una infraestructura compartida y dinámicamente escalable. Para más información, véase: https://uncitral.un.org/es/cloud

2 Incluye 1304 respuestas de los siguientes países: Brasil, Colombia, Costa Rica, México, Perú, Panamá y Uruguay. Para más información, ver anexo 1.

Dada la inexistencia actual de lineamientos y política pública en torno al manejo responsable de los datos de niños y niñas en ambientes digitales escolares, se vuelve una prioridad que cada escuela priorice el traslado del cuidado de datos que ha tenido en el mundo físico al mundo digital. Los resultados de la encuesta revelaron que solo 13,9% de las instituciones educativas se comunica con la aplicación correspondiente para eliminar los datos de sus estudiantes una vez que dejan de utilizarla, lo que significa que 86,1% no tiene procedimientos para la eliminación de datos o los docentes no conocen si existe uno para hacerlo.

Esta transición abrupta al mundo digital dejó en claro que docentes y directivos necesitan toda la ayuda necesaria para permitir la continuidad en la enseñanza, sin comprometer la seguridad de los datos de sus estudiantes. 72,3% de los docentes no cuentan con capacitación (o esta es insuficiente) para temas de privacidad de datos y uso responsable de plataformas y herramientas digitales, lo que significa que solamente el 14,9% ha recibido capacitación reglamentaria o considera que esta ha sido suficiente.

Por esta razón se aliaron el Grupo BID[3] y el Laboratorio de Resiliencia Eón de C Minds[4], bajo la iniciativa fAIr LAC[5], para diseñar e implementar el proyecto de Aprendizaje en línea seguro, que nació con el objetivo de responder a la urgente necesidad de la protección de datos digitales de niñas y niños en ambientes educativos. Como parte de este proyecto, se diseñó esta Guía para el personal directivo y docentes que buscan fortalecer la protección de los datos de sus estudiantes en las plataformas en línea que usan en y para las instituciones educativas.

La Guía se divide en dos secciones: la sección teórica informativa, donde se analizan los riesgos y los conceptos relevantes para identificar los riesgos a los que se enfrentan las instituciones educativas y colegios en línea, y la sección con recomendaciones de buenas prácticas, para que las instituciones educativas cuenten con las herramientas para proteger los datos de estudiantes y docentes, pues las instituciones educativas, aun cuando contraten con terceros el uso de plataformas educativas en Internet, siguen siendo las responsables del servicio educativo, mientras que las empresas se encargan del tratamiento.

En este sentido deben seguir atendiendo todas las conocidas prerrogativas, directrices y normativas aplicables al tratamiento de los datos, conforme al marco legal, tales como:

- Conservar los datos personales solo por el plazo estrictamente necesario para cumplir la finalidad de su uso, estableciendo plazos para eliminación de datos.
- Recabar datos adecuados, pertinentes y limitados a las finalidades para la cual son solicitados.
- Adoptar medidas técnicas y organizativas como la seudonimización, cifrado de datos, garantía de confidencialidad, integridad, disponibilidad de los sistemas, medidas de continuidad en caso de incidentes y procesos de evaluación o verificación periódica de las medidas de seguridad para el tratamiento de los datos.

3 Para más información, véase https://www.iadb.org/es/acerca-del-bid/financiamiento-del-bid/financiamiento-del-bid%2C6028.html

4 Para más información, véase https://www.cminds.co

5 fAIr LAC es una alianza entre los sectores público y privado, la sociedad civil y la academia para incidir tanto en la política pública como en el ecosistema emprendedor en la promoción del uso responsable y ético de la IA. Más información en https://fairlac.iadb.org/es

2. Breve resumen del contexto en Latinoamérica

Según UNICEF-UNESCO (UNICEF, 2020), más de 70 % de los países en Latinoamérica decidieron migrar a plataformas en línea para la educación a distancia a nivel básico y medio. A pesar de que en la región existe una cultura de seguridad (BID y OEA, 2020), es posible que en varios casos la premura de la adopción tecnológica no haya permitido implementar lineamientos y protocolos de ciberseguridad.

En materia de protección de datos, Latinoamérica tiene retos específicos en el entorno educativo. Solo en el último año, 67% de las instituciones educativas ha sido víctima de ciberataques[6] y apenas 44 % (ESET, 2017) de estas cuenta con medidas básicas de protección. La encuesta regional reveló que únicamente 5,8% de los docentes saben si su institución cuenta con un protocolo en caso de violación o filtración de datos; de esa cifra, el 25% de los docentes ignora cómo se lleva a cabo este protocolo.

En contraste, de acuerdo con la Agencia de la Unión Europea para la Ciberseguridad (ENISA), 80% de las instituciones educativas (OAS, 2020) en la Unión Europea cuenta con medidas básicas de protección.

3. Metodología

Con el objeto de hacer un diagnóstico del estado, las necesidades, los retos y oportunidades alrededor de la protección de datos digitales de estudiantes en ámbitos escolares de Latinoamérica, además de la investigación documental, se llevaron a cabo tres actividades en el marco del proyecto **Aprendizaje en línea seguro**: (1) entrevistas semiestructuradas individuales, con 15 personas expertas; (2) dos conversatorios regionales con docentes de cuatro países y (3) la encuesta regional en donde participaron 1304 directivos y docentes de siete países[7].

Para conocer más acerca de la metodología y estas colaboraciones ver el anexo 1 de esta Guía.

6 Ver Glosario para la definición de ciberataque.

7 Los países encuestados fueron: Brasil, Colombia, Costa Rica, México, Panamá, Perú y Uruguay.

II. Ciberseguridad en la institución escolar

Esta sección explora algunas preguntas cruciales en torno a privacidad y seguridad en las plataformas educativas digitales a las que docentes y directores pueden enfrentarse en la transición digital de los ámbitos educativos. Conocer estos conceptos ayuda a visibilizar los riesgos en línea para la protección de los datos de sus estudiantes y la importancia de esa protección.

1. ¿Qué son las plataformas educativas digitales?

Las plataformas educativas son programas de Internet[8] para conectar y comunicar con estudiantes, docentes, directores y padres de familia de una misma organización escolar. Estas plataformas pretenden ofrecer una experiencia digital similar a la que se tiene dentro de una institución educativa. Por ello, la mayoría de las veces incluyen funciones como herramientas de comunicación interna (foros, chats y plataformas para videollamadas); funciones de gestión de acceso que permiten que cada usuario pueda acceder solo a las áreas y funciones que les corresponden y sistemas de evaluación (hay plataformas que permiten subir y mostrar calificaciones e incluso algunas tienen evaluaciones automatizadas, entre otras funciones).

2. ¿Qué ocurre cuando accedemos a plataformas educativas en línea? ¿Existe un registro de la actividad en línea de estudiantes y docentes?

Dicho de manera simple, cada vez que accedemos a Internet generamos datos digitales y estos se registran en los servidores que usa la plataforma a la que accedemos. Cada acción que realizamos en línea se convierte en un dato digital. Toda esa información que se genera como resultado de la actividad en línea de una persona o, en otras palabras, toda la información que existe en Internet sobre una persona como resultado de su actividad en línea, se conoce como su huella digital.

Los datos provienen de las búsquedas que realiza una persona, de las páginas que visita y con las que interactúa y del uso de plataformas digitales. Es importante que la plantilla educativa tenga conciencia de que, al trasladar la educación al mundo digital, está contribuyendo a la creación y/o al crecimiento de la huella digital de niñas y niños, huella que puede incluir información privada, sobre todo cuando las plataformas conservan información para perfilar a los usuarios y segmentarlos con propósitos comerciales o de otro tipo.

8 Internet es un sistema de comunicación entre millones de dispositivos electrónicos. Internet se compone de dos actores principales: los servidores y los proveedores.

3. ¿Un tercero puede acceder a la huella digital de sus estudiantes?

Las plataformas de terceros, ciertas páginas y plataformas web, así como diversas aplicaciones, suelen recolectar datos de los usuarios, incluso de manera automática (LSE, 2021), a veces sin notificar al usuario. Al visitar sitios web o usar aplicaciones existen cookies; estas son pequeñas piezas de datos almacenadas en la computadora del usuario, que rastrean y registran lo que hace en línea, desde analizar compras e ingresos económicos, hasta predecir comportamientos para desarrollar productos o mejorar productos existentes con base en sus preferencias.

Las cookies, aunadas con el ecosistema completo en línea que cruza información, posibilitan que un tercero externo acceda a la huella digital de los estudiantes si no se tiene cuidado con los sitios que visitan o la manera como comparten información. Organizaciones alrededor del mundo han explorado lineamientos sobre la buena gestión de datos. Un recurso pionero en la materia es el recurso de "Gestión ética de los datos"[9] de fAIr LAC.

4. ¿Por qué debe protegerse la huella digital de sus estudiantes?

Como espacio seguro, la institución educativa tiene la obligación de resguardar los datos que, físicamente, se almacenaba en las instituciones. Este deber se extiende actualmente a los datos digitales personales que conforman en parte la huella digital de los estudiantes para protegerlos en cuanto a su integridad y privacidad.

Dado que los docentes hacen uso de plataformas educativas y lúdicas para dar sus clases, es importante conocer que además de usar los datos recolectados por las cookies para fines de mejora de oferta, algunas de estas plataformas pueden vender dichos datos a compañías para personalizar la publicidad mostrada en línea, de acuerdo con los intereses específicos de cada usuario, así como para diseñar productos. Esto puede suceder en páginas web y aplicaciones utilizadas por los docentes para dar sus clases o por los estudiantes como parte de sus actividades escolares, sin que se sepa quiénes tienen acceso a los datos.

Usar plataformas de terceros sin precaución podría originar la difusión indebida de información confidencial, es decir, podrían hacer públicos datos privados, tales como el contexto socioeconómico o la salud mental y física de un estudiante. Más adelante se presentan recomendaciones sobre cómo tener el cuidado apropiado.

9 Para más información, véase: https://fairlac.iadb.org/es/gestion-etica-datos

5. ¿Cuáles son los principales riesgos a los que se enfrentan estudiantes, docentes y directores en la educación digital?

Siete tipos comunes[10] de riesgos de *bullying* y violencia que pueden enfrentarse los estudiantes en línea son: ciberacoso, amenazas por correo electrónico, *flaming*, *outing*, *phishing*, acoso por externos y usurpación de identidad.

A. Ciberacoso

El ciberacoso puede llegar a ser más intenso que el acoso en persona: es el acoso escolar que ocurre a través de medios electrónicos (correos personales o escolares, chats de las plataformas de videollamadas, plataformas educativas, redes sociales, etc.). En la mayoría de los casos, el ciberacoso permite un anonimato que los acosadores no tendrían en la vida física, lo que les permite agresiones más severas y continuas que aquellas que los estudiantes podrían recibir personalmente. Las amenazas, la forma más agresiva de ciberacoso, explicitan que el receptor sufrirá un daño físico o social a menos que cumpla las exigencias del acosador.

B. *Ransomware*

Por otro lado, las instituciones pueden ser víctimas de *ransomware*, situación en la que cibercriminales secuestran datos valiosos y extorsionan a la persona o institución para obtener un beneficio económico a cambio de dicha información. Según la Agencia Federal de Investigación (FBI) de Estados Unidos, el *ransomware* es una tendencia al alza en las instituciones educativas (Gobierno de Estados Unidos, 2020).

C. *Flaming*

Cuando una persona insulta o agrede a otra persona en discusiones exageradas o acaloradas en un foro online, puede producirse el *flaming* —acoso y ofensa llevados a un nivel extremo en público—. Si bien controlarlo es relativamente sencillo en plataformas escolares, es necesario considerar que este riesgo puede existir en espacios fuera del control de las instituciones educativas. El riesgo es más alto si las instituciones educativas redirigen a los estudiantes a un espacio, medio o plataforma que cuente con una sección de comentarios abierta al público, donde se puede comentar de manera anónima; por ejemplo, cuando se manda como tarea mirar un video de una plataforma externa a la de la institución escolar.

D. *Outing*

El *outing* es el acto de hacer pública una información compartida en privado (a través de correos electrónicos, fotos, textos u otras comunicaciones). El *outing* es especialmente hiriente cuando se hace en el contexto de la sexualidad o la orientación sexual, porque empuja a los adolescentes a hacer pública, de manera involuntaria, información que es privada.

10 Selección basada en el estudio de la UNESCO, *School violence and bullying: global status report*, y la guía de telecomunicaciones del gobierno de México, Informe Safe Kids Online Uruguay de UNICEF, entre otros documentos internacionales.

E. *Phishing*

El *phishing* es un ciberataque en el que el atacante se hace pasar por una entidad o persona de confianza, utilizando ingeniería social y medios electrónicos falsos para robar datos privados como, por ejemplo, el número de la tarjeta de crédito. Su objetivo es engañar al destinatario para que crea que el mensaje es algo que quiere o necesita. Esto refiere a que es posible que una persona se haga pasar por estudiante o docente para poder engañar a los alumnos.

F. Acoso por externos

Al tener los estudiantes una fuerte presencia en línea es posible que personas externas a la institución educativa puedan tener acceso a comunicación con los estudiantes y, en consecuencia, los hostiguen. El acoso en línea es cualquier tipo de abuso que ocurre en Internet, facilitado por la tecnología, como computadores, tabletas, teléfonos móviles y otros dispositivos con acceso a Internet[11].

G. Usurpación o simulación de identidad

Por el alcance tratado en esta Guía, la usurpación o simulación de identidad es la creación de un perfil falso o hacerse pasar por otra persona en redes, diciendo cosas vergonzosas, lascivas o malvadas con el fin de generar una mala imagen de ella en Internet.

11 El acoso puede ocurrir en cualquier lugar en línea que permita la comunicación digital, como redes sociales, mensajes de texto y aplicaciones de mensajería, correo electrónico y mensajería privada, chats en línea, comentarios en sitios de transmisión en vivo y chat de voz en los juegos, entre otros.

6. ¿Cuál es el riesgo de que terceros ajenos a la institución escolar accedan a los datos digitales de los y las estudiantes y el plantel?

El hecho de que las plataformas digitales vendan los datos obtenidos de las actividades educativas es, en varias ocasiones, ilícito, y desvirtúa la finalidad social de la enseñanza. Es alarmante que, para acceder a la educación, un niño o adolescente esté siendo constantemente vigilado al recopilar tanta información —privada, íntima y sensible— y mucho menos que se utilice para el bombardeo de anuncios publicitarios que nada tienen que ver con las actividades pedagógicas. Además, conviene recordar que en algunos países y en ciertas circunstancias la publicidad dirigida específicamente a los niños es abusiva (OCDE, 1999) y, por tanto, debería ser ilegal[12].

El riesgo de escuelas y colegios a ciberataques o recolección de datos es alto, dada la información personal que administran de estudiantes, docentes y todo el personal educativo. Las instituciones educativas suelen tener datos de documentos de identidad, historiales académicos, registros médicos, calendarios con horarios específicos, hasta datos financieros y de seguridad social, lo que conlleva un alto riesgo de acceso y robo de datos internos (ESET, 2017). Según el reporte de ESET en 2017 —el estudio de la región con el análisis más reciente—, 67% de las esas instituciones en Latinoamérica han sido víctimas de al menos un ataque cibernético[13].

Todo lo anterior no es motivo para rechazar las tecnologías. Las instituciones educativas pueden tomar acciones para mitigar los riesgos derivados de su funcionamiento en el entorno digital, así como asumir responsabilidades sobre la seguridad informática de su organización.

En la siguiente sección exponemos las prácticas que pueden implementarse para lograr que las instituciones educativas en línea sean seguras.

12 Casi ningún país latinoamericano penaliza esta acción en un Código legal. Un buen ejemplo de este tipo de leyes es la ley de Protección de la Privacidad en Línea (COPPA) de Estados Unidos, que aplica para la recopilación en línea de información personal por parte de personas o entidades bajo la jurisdicción estadounidense.

13 De acuerdo con la Organización para la Cooperación y el Desarrollo Económicos (OCDE), un ciberataque es un intento activo, malicioso y deliberado que hace una persona, grupo u organización para irrumpir en un sistema de información de cualquier persona, institución o Estado.

III. Buenas prácticas que pueden aplicarse en la escuela

Las siguientes acciones se dirigen a las instituciones educativas y su planta profesional. Estas recomendaciones se basan en mejores prácticas internacionales e incluyen todas las herramientas existentes a la fecha para que puedan adoptarlas las instituciones educativas con el fin de proteger los datos digitales de quienes estudian allí. Si bien la Guía se dirige principalmente a docentes y personas en roles directivos, también ofrece acciones que incluyen a padres y madres de familia y que también pueden tomar directamente los estudiantes.

A continuación, se presentan los tres actores que tienen un papel en garantizar la privacidad de los datos de los menores de edad en ámbitos escolares y un breve panorama de sus responsabilidades. Esta sección se divide en tres partes:

- Decisiones por tomar y buenas prácticas por adoptar a nivel de dirección, junto con los docentes dentro de la institución.
- Buenas prácticas de transparencia y comunicación constante de directores y docentes con padres, madres y estudiantes.
- Buenas prácticas para personal directivo, docentes y estudiantes.

Directivo/a (Di)	Docente (Do)	Padres de familia (Es)
• Principal responsable de la gestión escolar. • Cumple un papel central al articular la comunidad educativa. • Su labor es conducir y facilitar una serie de procesos dentro de la institución educativa.	• Brinda enseñanza y cuidado en el salón de clases. • Guía a los estudiantes en su proceso de aprendizaje. • Proporciona información relevante y oportuna.	• Líderes en el proceso de aprendizaje de los estudiantes. • Transmiten valores. • Se preocupan por la educación integral de sus hijos, incluyendo el plano de protección digital.

Las recomendaciones de las siguientes acciones compartidas se codifican con color, según el actor que debe implementarlas o seguirlas. Las recomendaciones tendrán un identificador naranja para directivos, amarillo para docentes y verde para padres de familia / estudiantes.

1. Decisiones por tomar y buenas prácticas por adoptar a nivel directivo y docente dentro de la institución

Esta sección cuenta con cinco apartados que ayudarán a los grupos directivos a establecer una buena gobernanza de datos dentro de su institución.

Di			A. Asignar a una persona o grupo de personas, según sea necesario, la responsabilidad de velar por el cumplimiento de tareas establecidas.

El derecho a la protección a la privacidad con respecto a los datos digitales de estudiantes comienza por su manejo responsable, conociendo el ciclo que siguen los datos en todas sus fases e identificando quién puede utilizarlos o tratarlos, para qué y por qué.

La institución educativa puede proteger la privacidad de la comunidad educativa al tener claridad de las plataformas usadas y designar a las personas encargadas de: a) cada una de las fases (recolección, almacenamiento, uso, acceso y eliminación) de los datos digitales y b) el uso de plataformas web propias de la institución educativa, así como externas.

El director:

a. Reparte las responsabilidades entre su personal para el manejo de datos digitales de estudiantes, docentes y todo el personal de la institución educativa. También puede considerar abrir nuevos puestos de trabajo para atender el tema de la privacidad. Podría ser un(a) encargado(a) de privacidad; por ejemplo, un(a) especialista en manejo de datos.

b. Establece procesos para el uso, selección y control de las plataformas web y aplicaciones que se utilizan en el ámbito escolar, tanto para dar clases en línea, como apoyar actividades educativas de los y las estudiantes para reforzar conocimientos, desarrollar habilidades, aprender jugando, etc.

c. Continúa aprendiendo para tener una gobernanza institucional correcta sobre los datos. Por ello, es recomendable estudiar recursos que plantean cómo escalar el impacto de una organización a través del uso de la tecnología, como el recurso de "Gestión ética de los datos"[14] de fAIr LAC.

d. Cuenta con protocolos o lineamientos sobre el buen uso de las tecnologías de la información y comunicaciones por parte de profesores, directivos y administrativos.

14 Para más información, véase: https://fairlac.iadb.org/es/gestion-etica-datos

El informe *Cost of a Data Breach Report 2020*, realizado por el Instituto Ponemon en conjunto con IBM, destaca que el tiempo promedio que tarda una organización a nivel global para identificar y contener una brecha de datos es de 280 días. En Latinoamérica, el tiempo promedio es de 328 días, lo que confirma que las organizaciones que no cuentan con controles que permitan detectar incidentes de seguridad con suficiente oportunidad no tendrán la capacidad de responder y contenerlos.

Esta situación es evidente en las instituciones educativas, que al no contar con mecanismos suficientes de monitoreo que les permitan identificar una brecha de datos o un ciberataque en progreso, de ninguna manera pueden afirmar que no está sucediendo y, en el mejor de los casos, solo podrían sostener que no lo saben.

Di			B. Implementar sistemas de seguridad en los dispositivos para evitar la fuga de datos o accesos no autorizados (ver anexo 2 para ejemplos).

Una de las maneras de prevenir la vulneración de la privacidad de los y las estudiantes, así como de toda la comunidad educativa de la que la institución educativa recolecta y usa datos, es a través de la adopción de sistemas de seguridad en los dispositivos que se usan con fines educativos. Para ello, es necesario:

a. Considerar la posibilidad de designar fondos para la instalación de dichos sistemas de seguridad, pues podría requerir presupuesto (ver anexo 2 para conocer algunos de los sistemas y herramientas de ciberseguridad que podrían implementarse en la institución educativa).

b. Tener en cuenta otras prácticas sencillas que mejorarán la seguridad y protección de privacidad:

   i. Asegurarse de tener y promover buenas prácticas de acceso, de tal manera que se utilice un mecanismo que permita la identificación de los y las estudiantes, tal como higiene de contraseñas y autenticación de doble factor o en dos pasos (ver anexo 3). Evitar aquellos procesos de autenticación que impliquen el uso de biometría (reconocimiento facial o huella dactilar), pues no es proporcional a las finalidades escolares. Las contraseñas de los correos y plataformas escolares son las llaves a la vida digital. Tomar las medidas apropiadas para contar con una contraseña robusta es clave para la protección de datos de estudiantes y del personal educativo (INCIBE, 2016)[15].

   ii. Algunas plataformas permiten configurar la aplicación de acuerdo con las políticas de contraseñas de la entidad educativa.

15 También hay otras buenas prácticas cíclicas en la Sección 3: Buenas prácticas para personal educativo, docentes y estudiantes, en la página 19.

Di			C. Crear un plan para gestionar la comunicación de una fuga de datos o accesos no autorizados.

Además de las debidas prácticas para la identificación, evaluación y gestión de riesgos y las políticas de prevención y mitigación de los mismos en torno a los datos digitales, también es recomendable crear un plan de respuesta ante las contingencias, que incluya protocolos que permitan asegurar la continuidad del negocio, estar preparados para el manejo de una falla de seguridad y responder ante un ciberataque y sus consecuencias.

En los siguientes cinco puntos puede encontrarse información relevante.

? ¿Cómo darse cuenta de si hubo una fuga de datos y cómo reaccionar?

Percatarse de una fuga es difícil, pues muchas veces se hace de manera silenciosa. Un elemento indispensable para detectar y responder de forma oportuna a un incidente de seguridad es el monitoreo de ciberseguridad, que debe otorgar visibilidad de los eventos que ocurren en la infraestructura tecnológica de la institución; por ejemplo, sus redes, sus plataformas virtuales o sus aplicaciones, es decir, que tenga la capacidad de detectar y vigilar los distintos elementos que recolectan, procesan, resguardan o transmiten información sensible de la comunidad educativa y de los sistemas o plataformas que soportan y habilitan la labor educativa (para más información, ver anexo 2).

Si la institución educativa ha tenido un incidente cibernético, no debe asumirse automáticamente que ha habido una violación de datos; y si ha tenido lugar una violación, puede o no ser notificable. Esto dependerá de los marcos regulatorios de cada país.

Un ejemplo de un estándar de regulación de protección de datos es el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Por lo general, para que una violación sea notificable a la autoridad de control debe existir un riesgo probable para los individuos (por ejemplo, el robo de datos de la nómina que podría conducir a pérdidas financieras).

Antes de entrar en más detalles sobre los rasgos clave de una violación de datos, se comparte a continuación un breve resumen:

1. Una violación de datos evoluciona con rapidez y requiere una respuesta igualmente rápida para evitar más pérdidas.
2. Hay muchas partes interesadas, lo que hace que la comunicación sea un elemento clave de cualquier plan de preparación para enfrentar la violación de datos.
3. La privacidad, la identidad o los intereses financieros del personal, los padres y los estudiantes del centro educativo pueden verse comprometidos en una violación de datos. Es responsabilidad del centro educativo proteger a los interesados.

4. A la hora de informar sobre una violación de datos (dependiendo de la región), se dispone de 72 horas para informar al organismo regulador. Aquí, el tiempo es todo.
5. Sin un plan en marcha, se está poniendo en riesgo a la comunidad y la reputación de la institución escolar.

¿Qué hacer si hay una fuga de bases de datos con información sensible?

Es importante actuar lo más rápido posible (INCIBE, 2012) durante todo el protocolo. Esta tabla indica la respuesta inmediata ante un incidente. El anexo 4 presenta un protocolo general de prevención y para evitar las situaciones de urgencia y emergencia.

Acciones	Paso a paso
1. Procurar la detección temprana del incidente siempre que sea posible, para dar inicio de inmediato al protocolo de acción correspondiente (ver anexo 4 para protocolo de respuesta ante incidentes).	a. Determinar cuáles son los datos afectados y su cantidad. b. Establecer la causa de la fuga, sea de origen técnico o humano.
2. Realizar el proceso de valoración inicial del incidente una vez que se conoce la información anterior y determinar los pasos que deben seguirse.	c. Determinar las acciones para cerrar la fuga y evitar nuevas fugas. d. Planificar el plan de comunicación del incidente y de los afectados, únicamente en caso de ser necesario según los datos vulnerados. e. Estimar el impacto: daño reputacional, legal, financiero o de otra naturaleza.
3. Ejecutar el plan de acción.	f. Terminar la brecha de seguridad, a través de la desconexión de un servicio o sistema, según el origen de la fuga de datos. g. En caso de que los datos se hayan hecho públicos, localizar en dónde están publicados y tomar acción para solicitar su eliminación inmediata. h. Informar a docentes, estudiantes, padres y madres acerca del incidente. En caso de haber sucedido una fuga de datos sensibles, informar también cuáles fueron los datos afectados para que puedan tomarse las acciones correspondientes para su seguridad.

¿Qué hacer si hay una intrusión no deseada en una clase virtual?

Junto con el aumento de uso de plataformas de videoconferencia, que han fungido como aulas virtuales ante la suspensión de las clases presenciales por COVID-19, surgió también el llamado *Zoombombing* (Consejo Escolar Conejo Valley, 2020), en el que personas no deseadas ingresan a las sesiones virtuales y muestran contenido inapropiado (pornográfico o racista, por ejemplo), sin importar que haya menores de edad. Enseguida aparecen algunas maneras de prevenir el riesgo y de mitigarlo, en caso de que suceda.

Prevención	Mitigación
- Utilizar una plataforma de videoconferencia que permita hacer ajustes de seguridad. - Asegurarse de que la videoconferencia sea privada, a través de una contraseña de reunión o sala de espera para permitir el ingreso manualmente. - No compartir el vínculo web o ID de reunión de manera pública, como en redes sociales. De preferencia generar una contraseña única para cada reunión. - Configurar la sesión para que solo una persona designada pueda compartir pantalla. De esta manera si alguien indeseado ingresa, no podrá mostrar ningún video o imagen en la pantalla principal. - Realizar simulacros de manera periódica en la escuela. Así puede asegurarse de que todos los docentes están preparados en caso de que una persona indeseada entre a su clase en línea.	- En cuanto se identifique que hay una persona no deseada en la sesión virtual, el anfitrión o la persona designada para controlar los permisos en una videollamada, tendrá que expulsar cuanto antes al intruso. - Para sacar a personas no deseadas algunas plataformas permiten eliminar participantes no deseados de la sesión. En el menú *Participantes* se pone el puntero sobre el nombre del participante que quiera eliminarse, para que se muestren varias opciones de acciones que llevar a cabo, tal como *Eliminar*. Al dar clic, lo saca de la sesión. - Si toma tiempo identificar a la persona no deseada, lo recomendable es finalizar la videollamada.

¿Cómo informar a padres, madres y estudiantes afectados cuando sucedió una falla de seguridad?

Las fallas de seguridad pueden causar daños en la imagen de la institución escolar, además de poner en riesgo a estudiantes y docentes. En caso de haber sucedido una fuga de datos sensibles, es importante avisar a padres, madres y estudiantes, informándoles cuáles fueron los datos afectados para que puedan tomar las acciones correspondientes para su seguridad (consultar en el anexo 5 la base para protocolo de informe sobre incidente).

¿En qué casos informar a las autoridades?

Si la falla de seguridad en cuestión vulnera de manera grave datos de carácter personal que pudieran afectar la integridad del estudiante, sería necesario comunicar el incidente a "fuerzas y cuerpos de seguridad, ya sean locales, regionales o nacionales, en función del escenario. Por otro lado, se llevará a cabo la denuncia del incidente y otras acciones que puedan derivarse de la coordinación de la solicitud de información por parte de las fuerzas y cuerpos de seguridad" (INCIBE, 2012).

También hay que tener en cuenta la posibilidad de informar a organismos y autoridades correspondientes que puedan tener competencias derivadas de la información filtrada, como oficiales de protección de datos (Arias Ortiz y Cristia, 2014) designados en organismos gubernamentales, el área correspondiente del Ministerio de Educación o según lo establecido en la legislación de cada país.

Di			D. Seleccionar las herramientas permitidas para la comunicación digital entre docentes y estudiantes (lineamientos del director).

Las instituciones educativas requieren servicios y productos de terceros, indispensables para la educación en línea. Sin embargo, en la medida de lo posible, es responsabilidad de la institución educativa asegurarse de que esos productos y servicios que deciden utilizar tengan las protecciones apropiadas para los datos de sus estudiantes, es decir, que cuenten con garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento que hagan sobre los datos esté conforme con el marco normativo que aplique.

¿Cuáles serían los criterios de selección de una plataforma en términos de privacidad y seguridad?

Antes de utilizar cualquier servicio tecnológico, ya sean plataformas, páginas web o aplicaciones, con los y las estudiantes o que involucre sus datos, es necesario leer los Términos o condiciones de uso y la política de privacidad[16] o, en su caso, el contrato que se celebre, y asegurarse de la existencia de ciertas garantías, como estas:

- Los datos se tratarán únicamente conforme a las instrucciones de la institución escolar.
- No se utilizarán los datos para finalidades distintas a las acordadas.
- Se detallarán medidas de seguridad para la protección de los datos.
- Se devolverán o eliminarán los datos una vez finalizado el contrato o el uso de la plataforma.

16 El contenido de aviso de privacidad varía de país a país. Es necesario verificar la regulación nacional antes de aceptar los términos y condiciones.

A pesar del lenguaje legal o técnico que suelen utilizar estos documentos digitales, aceptarlos antes de usar un servicio es similar a firmar un contrato, el cual involucra ciertas obligaciones e incluso cede ciertos datos, por lo que es necesario que padres, madres de familia y docentes estén enterados de lo que involucra utilizar un servicio. El anexo 6 contiene varias preguntas que facilitarán la lectura de los Términos o condiciones de uso y política de privacidad para resaltar los criterios que deben tenerse en cuenta al seleccionar servicios tecnológicos de uso escolar y garantizar la protección de la privacidad y seguridad de los datos digitales de sus estudiantes.

¿Cuáles son la(s) plataforma(s) y herramienta(s) de comunicación autorizada(s) por la institución escolar?

Una vez revisados los criterios óptimos de selección de un servicio digital para uso escolar lo recomendable es que la institución educativa cuente con una lista oficial de las plataformas y herramientas de comunicación autorizadas entre docentes y estudiantes (ver anexo 7 para encontrar un análisis de plataformas existentes). Esta lista sería pública para que todos en la comunidad educativa padres, madres, docentes y estudiantes conozcan cuáles son las plataformas y aplicaciones permitidas y se limiten a que estos últimos solo usen esos servicios tecnológicos, lo que permitirá a la institución educativa un mejor control para la protección de los datos digitales estudiantiles, así como el manejo de riesgos en caso de generarse alguna afectación.

Además, deberá proporcionarse, a padres de familia y tutores, información básica, clara y concisa sobre los términos y características de los servicios contratados, finalidades del tratamiento de los datos y políticas de privacidad y protección de dichos proveedores. Dependerá de cada legislación si es necesario contar con un nuevo consentimiento, pues algunos padres pudieran no saber con claridad cuáles son los datos de sus hijos que pueden recolectarse o deducirse a través de las plataformas, ni el uso que puede llegar a dárseles.

Di			E. Adaptar el reglamento de la institución educativa para incluir temas digitales.

Dado que el uso de plataformas digitales está inmerso en el día a día escolar es importante incluir temas específicos en el reglamento de la institución educativa para que haya lineamientos claros y pueda comenzar a crearse un espacio digital seguro para sus estudiantes, así como para todo el personal escolar. El anexo 8 brinda sugerencias de secciones que pueden incluirse en el reglamento escolar con respecto a temas digitales.

Es importante que en este reglamento se establezcan reglas y penalizaciones para aquellos estudiantes que incurran en actividades como *ciberbullying*, *outing* o *flaming*, antes de que ocurra cualquier incidente.

2. Buenas prácticas de transparencia y comunicación constante de directores y docentes hacia padres, madres y estudiantes

Si bien es importante que la institución educativa tenga todas las medidas posibles para protección de la seguridad y privacidad de los datos digitales de sus estudiantes, también es una labor que requiere comunicación constante y transparencia con toda la comunidad educativa, incluidos estudiantes, padres y madres, con respecto a la recolección, uso, almacenamiento, manejo y eliminación de sus datos. Para esto pueden llevarse a cabo las siguientes buenas prácticas que permitirán mantener informada de manera pertinente a la comunidad educativa y marcar una diferencia en el uso y manejo ético de datos.

Di	Do	
		A. Requerir la firma (física o digital) del reglamento: actualizado con temas digitales por parte de los padres de estudiantes menores de edad y por parte de estudiantes mayores de 18 años. Se recomienda una firma general por parte del director y una por salón por parte del docente.

Carta de notificación a padres y madres

Además de contar con el reglamento escolar actualizado en temas digitales, este debe integrar los protocolos de emergencia para que padres y estudiantes estén enterados. Un protocolo sirve para seleccionar las plataformas web y aplicaciones para uso en el ámbito escolar y es recomendable tener una lista oficial de ellas. También es importante resaltar el tema de notificación y consentimiento cuando se trata de datos digitales. Para el uso de plataformas web y aplicaciones que requieran datos de estudiantes se recomienda contar con una carta de notificación a padres y madres acerca de qué tipo de datos digitales recolectan las herramientas tecnológicas que utilizarán sus hijos en cualquier actividad escolar.

Contar con un análisis previo de las plataformas web y de las aplicaciones autorizadas por la institución escolar facilitará conocer los detalles de los datos digitales que se recolectan para notificar a padres y madres. En el anexo 9 se encuentra una propuesta de carta de notificación para estos casos.

Capacitación continua y campaña de información sobre el tema

La adquisición de habilidades para habitar un mundo digital ya no es un tema optativo. Tanto docentes como estudiantes requieren un fortalecimiento constante acerca de los riesgos para los datos digitales que este mundo conlleva. Es recomendable establecer plazos (mensuales, semestrales o anuales) para tener capacitación continua, tanto del personal educativo directores(as), docentes y estudiantes hasta sesiones informativas para padres y madres con el propósito de concientizar acerca de la importancia de proteger los datos digitales.

Esta capacitación puede reforzarse con una estrategia de comunicación sobre temas de protección de datos digitales que inviten a la reflexión e informen acerca de los riesgos y

cómo mitigarlos. El anexo 10 ofrece recursos de apoyo a administradores y docentes para realizar actividades y talleres con estudiantes, padres y madres.

Una estrategia de comunicación cuyo objetivo sea informar la importancia de la protección de datos digitales es un paso importante para la conscientización del tema. Una campaña de información de esta índole debe dirigirse a estudiantes, padres y madres, pues estos últimos tienen una labor importante en el seguimiento del aprendizaje de sus hijos, pues el uso digital ha aumentado con la transición a lo virtual que trajo consigo el COVID-19 (UNICEF, 2020b). El anexo 11 menciona las temáticas relevantes para armar una campaña de información sobre el tema.

Después de que reciban la capacitación, los y las estudiantes deberán ser capaces de:

1. Reconocer un correo que no es institucional.
2. Evitar entablar conversaciones en Internet con personas desconocidas.
3. Respetar a los demás en los espacios en línea.
4. Reconocer cuando no deben compartir información en plataformas no autorizadas.
5. Saber reconocer un sitio que contiene información legítima.

3. Buenas prácticas para personal directivo, docentes y estudiantes

En el numeral III, 1 se abordaron recomendaciones de decisiones de alto nivel que debe tomar el personal directivo. Las siguientes recomendaciones son acciones orientadas a ese personal, a docentes y a estudiantes.

Di	Do	Es	
			Asegurarse de que el personal directivo, docentes y estudiantes adopten las mejores prácticas periódicas en los dispositivos de uso escolar.

Además de las buenas prácticas dentro de la institución escolar y las destinadas a informar a estudiantes, padres y madres, hay una serie de prácticas cíclicas que se recomienda tener en cuenta al navegar en línea. Son prácticas sencillas de realizar desde las escuelas y colegios, pero también hay que invitar a que estudiantes, padres y madres las lleven a cabo como medidas de protección de los datos digitales.

A continuación, aparecen las mejores prácticas cíclicas en torno a navegación digital, plataformas web y aplicaciones para una mayor protección de los datos.

Actualizar los sistemas operativos y los programas instalados

Mantener actualizados los sistemas operativos y las aplicaciones de los dispositivos en la escuela o colegio, así como los antivirus y las versiones de los navegadores, porque las actualizaciones normalmente incluyen cambios importantes que mejoran el rendimiento y la seguridad de los equipos. Muchos de estos lo realizan de manera automática; únicamente es cuestión de aceptar esa actualización en el momento que se notifica. Por lo mismo, también debe informársele a la comunidad escolar, docentes, estudiantes, padres y madres acerca de la importancia de hacerlo en las computadoras personales, celulares y tabletas que usen estudiantes y docentes en sus casas (Gobierno de México, 2020).

Hacer copias de seguridad

Realizar copias de seguridad periódicas de los datos es una medida que debería de extenderse (INCIBE, 2017) en todas las instituciones educativas. Esto permitirá recuperar datos en caso de que haya alguna pérdida.

Para realizar copias de seguridad hay que:

- Identificar los datos que se requiere preservar.
- Establecer la frecuencia de los procesos de copia y contar con dispositivos de almacenamiento.
- Controlar el acceso a los dispositivos de almacenamiento de las copias.

Cambiar las contraseñas

Además de tener contraseñas robustas (ver anexo 3), se recomienda cambiarlas periódicamente, pues los hackers tienen maneras de descifrarlas, por lo que el cambio con frecuencia brinda mayor protección. Por esto, desde las instituciones educativas es importante establecer un periodo de renovación de las contraseñas, especialmente en aquellos sitios o servicios que contengan datos estudiantiles.

Eliminar historial y cookies

Sabiendo que las cookies almacenan datos acerca de nuestra navegación en Internet es recomendable borrarlas al terminar de usar el navegador o establecer una fecha para hacerlo periódicamente.

- Si hay abierta cualquier página web, la combinación de teclas Ctrl + Mayus + Supr abre directamente la ventana para borrar datos de navegación.
- Otra manera de eliminar esos datos depende del navegador que se utilice. En el anexo 5 se encuentran recomendaciones.

Verificar que la dirección electrónica señale "HTTPS"

Se puede adoptar el Protocolo de transferencia de hipertexto (*HyperText Transfer Protocol Secure* o HTTPS, por sus siglas en inglés), un protocolo de Internet que protege las conexiones de los usuarios en los sitios web, de manera que la experiencia en línea sea segura y privada. Esto implica varios pasos que pueden explorarse en esta página[17].

Tomar precauciones al usar computadoras compartidas

Las computadoras compartidas pueden encontrarse en distintos tipos de entornos: una computadora compartida en hogares, instituciones educativas e incluso en librerías públicas o cafés internet. Para usarlas de manera segura y sin compartir información confidencial de forma accidental con los usuarios que continúen su uso, se recomienda:

- Nunca guardar contraseñas que se completan de manera automática, ni pulsar "recordar".
- Siempre cerrar sesión en todos los sitios donde se haya ingresado.
- De preferencia, utilizar el "modo incógnito".
- Evitar usar las computadoras compartidas para realizar trámites que impliquen emplear información personal o sensible (una transferencia bancaria, formularios de centros médicos, etc.).

Implementar controles parentales

Una herramienta que puede ayudar a la seguridad de niños y niñas en línea es el control parental, el cual sirve para cuidar la navegación por Internet, manteniéndolos alejados de contenido inapropiado. Los implementadores de este control —docentes, padres, madres o tutores— podrán bloquear ciertos sitios web y categorías de información, además de restringir las descargas. Este último punto aumenta la seguridad del dispositivo ante software malicioso (también conocido como malware) y virus. Se recomienda en particular para niños menores de 14 años (Grupo Ático, 2020).

Algunos controles parentales pueden rastrear las conversaciones en diversos sitios web, contribuyendo así a combatir el ciberacoso.

Usar redes Wi-Fi en forma segura

Con las clases en línea se vuelve aún más urgente la recomendación de aplicar medidas de seguridad para las redes en los hogares de los estudiantes. Asegurarse de que la red Wi-Fi requiera una contraseña cada vez que un nuevo dispositivo se conecta por primera vez ayudará a evitar que usuarios no autorizados ingresen a la conexión (Gobierno de España, 2021).

A la vez, se recomienda evitar el uso de redes Wi-Fi públicas para compartir contenido sensible, pues otros dispositivos conectados a la misma red pueden capturar la información transmitida.

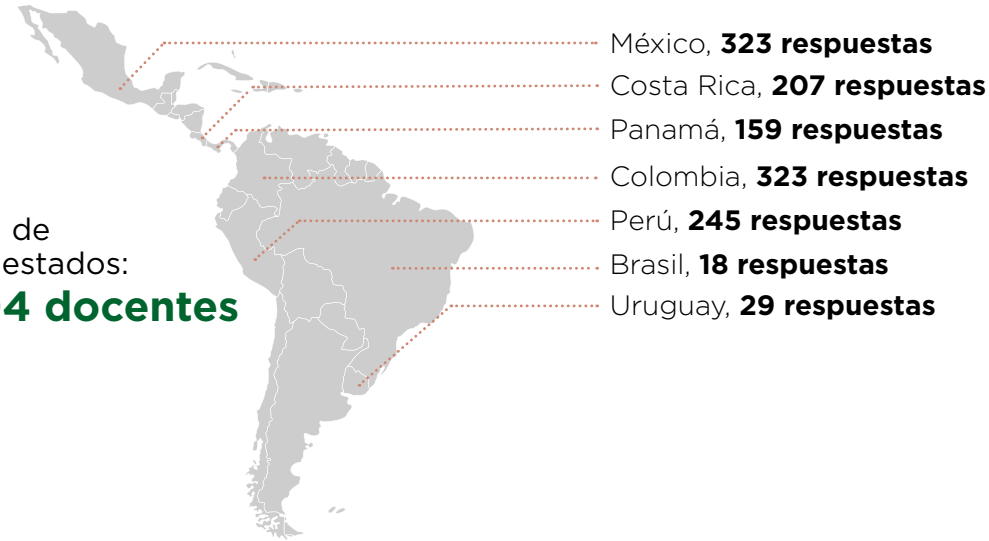
17 Para más información, véase: https://developers.google.com/search/docs/advanced/security/https?hl=es

Anexos

Anexo 1. Metodología

1. Encuesta regional para docentes

Como parte de las actividades de investigación para este proyecto se creó la ***Encuesta Aprendizaje en línea seguro LATAM***. La encuesta buscó entender el nivel de información que tienen docentes y directores sobre el tema de privacidad de datos de niñas y niños en ámbitos escolares. Se encuestaron más de 100 docentes de siete países[18] de Latinoamérica. Esta es la única encuesta de su tipo en la región y sirvió como insumo para seleccionar el contenido relevante en esta Guía.



2. Conversatorio con docentes y personal directivo latinoamericano

Se realizó un conversatorio con docentes de Argentina, Ecuador, México y Perú para entender los retos a los que se enfrentaban en la transición digital, sus experiencias y preocupaciones para integrarlas en esta Guía. Las personas participantes se encuentran en la sección de Agradecimientos al inicio del documento.

3. Entrevistas con personas expertas en temas de educación, sistema educativo y privacidad en Latinoamérica

Como parte del proyecto ***Aprendizaje en línea seguro*** se realizaron 15 entrevistas con personas expertas en temas de educación, sistema educativo y privacidad en Latinoamérica e internacionalmente para conocer mejores prácticas, retos actuales y consideraciones de alto nivel. Las personas participantes se mencionan en la sección de Agradecimientos al inicio del documento.

18 Total de encuestados: 1304 docentes, así: Brasil, 18 respuestas; México, 323 respuestas; Colombia, 323 respuestas; Costa Rica, 207 respuestas; Panamá, 159 respuestas; Perú, 245 respuestas, y Uruguay, 29 respuestas.

Anexo 2. Recomendaciones de sistemas y herramientas de ciberseguridad

a) Ciberseguridad organizacional

1. Monitoreo preventivo[19]

Se puede entender el monitoreo de ciberseguridad como el proceso clave en la detección oportuna de ciberamenazas y brechas de datos para responder antes de que estos causen daños o disrupción a mayor escala. Es importante que la institución educativa decida si lleva a cabo este proceso internamente o si contrata el apoyo de un tercero especializado.

En ambos casos, la institución deberá asegurarse de que el personal encargado cuente con:

- Claridad en su rol, funciones y el tiempo necesario para realizar esta actividad.
- Capacitación suficiente para la interpretación de eventos con el fin de determinar la gravedad de incidentes de seguridad.
- Capacitación propia del fabricante de la solución de monitoreo elegida (en caso de que aplique).
- Procesos y protocolos claramente definidos, descritos e implementados para notificar, escalar y responder a un incidente de ciberseguridad.
- Soporte del fabricante en caso de falla en la solución, o asesorías sobre dudas de los eventos que se identifiquen.

En cualquiera de las opciones anteriores, es importante realizar una adecuada selección de la solución de monitoreo de ciberseguridad. A continuación, se enlistan algunos criterios que conviene tener en cuenta:

- Visibilidad en tiempo real.
- Priorización de amenazas.
- Analítica de datos.
- Notificaciones automáticas.
- Alimentación por fuentes de inteligencia.
- Integración con otras plataformas de redes o seguridad.
- Creación de una base para protocolo de respuesta ante incidentes.

Antes de compartir información con terceros, es importante que las instituciones educativas consideren las prácticas de datos de los proveedores de servicios para mantener la confidencialidad y seguridad de los datos y prevenir el acceso o uso no autorizado de la

19 Esta sección fue redactada con insumos de Capa 8, Escuelas Ciberseguras. Para más información ver: https://capa8.com/

información. Es importante que estos terceros sean capaces de mantener la confidencialidad y seguridad de la información, particularmente cuando se trata de datos de menores de edad. A su vez, se recomienda que la institución educativa realice contratos de privacidad de datos con cualquier tercero que tenga acceso a ellos, como indica la Ley de Protección de la Privacidad en Línea para Niños (en inglés: Children's Online Privacy Protection Act (COPPA)) de Estados Unidos.

b) Ciberseguridad técnica

1. Protección en la conexión de la red: cortafuegos (firewall, en inglés) para todo equipo de uso escolar

Se recomienda activar funcionalidades de protección, como los cortafuegos (firewall), incorporadas en los sistemas operativos más comunes. Un cortafuegos es la primera línea de defensa ante un ataque desde la red y protege el equipo de programas maliciosos o de atacantes que intenten conectarse al equipo en forma remota. Además, permite establecer reglas para indicar qué conexiones de red deben aceptarse y cuáles no.

Los sistemas operativos como Windows, Mac[20] o Linux incluyen cortafuegos gratuitos.

2. Protección de los dispositivos: antivirus

Es importante instalar y mantener actualizado un antivirus en todo dispositivo electrónico, porque es la única manera de detectar y destruir un virus; este puede encontrarse en la computadora si se ha descargado contenido de Internet.

- Dos antivirus no implican mayor seguridad, por lo que se recomienda invertir en un antivirus que ofrezca garantías considerables de seguridad.
- Al instalar y actualizar antivirus se recomienda hacerlo desde el sitio web oficial y nunca descargarlo de un sitio de dudosa procedencia.

20 Los equipos de Mac cuentan con un cortafuegos de alto rendimiento, por lo cual podría creerse (SAIGAL, 2020) que no se necesita descargar uno, pero es aconsejable tener doble protección.

Anexo 3. Protocolo de buenas prácticas de acceso: higiene de contraseñas y autenticación de doble factor

De acuerdo con la Oficina de Seguridad del Internauta (OSI) del Instituto Nacional de Ciberseguridad (INCIBE), hay cuatro características para que las contraseñas sean lo más seguras posible.

Se recomienda que las contraseñas sean:

1. **Secretas.** Compartir las contraseñas con otras personas vulnera la seguridad de la información, pues alguien más tendría acceso a esta.

2. **Robustas.** Una contraseña con medidas robustas protege nuestra privacidad en mayor grado, porque dificulta que otro acceda a ella. Según el OSI de INCIBE[21], la contraseña debe:

   - Tener una longitud mínima de ocho caracteres.
   - No contener su nombre, ni el nombre de su usuario, ni el del colegio donde estudia o trabaja, ni parte de los mismos.
   - No contener palabras del diccionario.
   - No incluir información personal: fecha y/o lugar de nacimiento, número de documento de identidad, número de teléfono, fechas especiales, etc.
   - No formarse con números y/o letras que estén adyacentes en el teclado.
   - Contener caracteres de cada uno de los siguientes grupos: letras mayúsculas, letras minúsculas, dígitos y caracteres especiales.

3. **Únicas para cada sitio o servicio.** Utilizar la misma contraseña para todos los sitios o servicios que usamos implica mayor vulnerabilidad de nuestra privacidad, pues si alguien descifra la contraseña permitiría su acceso a todas nuestras cuentas. Basta con hacer una ligera variación sobre la base de la contraseña para cada sitio, de manera que no se vuelva muy complicado memorizarlas.

4. **Cambiadas periódicamente.** Como los hackers tienen maneras de descifrar contraseñas, es recomendable cambiarlas periódicamente. En el caso de las instituciones educativas, es especialmente importante establecer un periodo de renovación de las contraseñas en aquellos sitios o servicios que contengan datos estudiantiles.

Además, siempre que sea posible, se recomienda utilizar la verificación o autenticación en dos pasos o la autenticación multifactor (MFA, por sus siglas en inglés). Es un sistema de seguridad que requiere más de una forma de autenticación para verificar la legitimidad de una transacción. El objetivo de la MFA es crear una defensa por capas y hacer que sea más difícil para una persona no autorizada acceder a un objetivo, como una ubicación física, un

21 Para más información véase: https://www.osi.es/es/actualidad/blog/2013/12/05/creando-contrasenas-robustas

dispositivo de cómputo, una red o una base de datos. En otras palabras, si uno de los factores se compromete o se rompe, el atacante todavía tiene al menos una barrera más que romper antes de ingresar con éxito en el objetivo.

En particular, la autenticación en dos pasos da una mayor protección contra accesos no autorizados a una cuenta, ya que además de la contraseña se debe ingresar un código. Este código llega por correo electrónico, generado en una app, o por mensaje de texto SMS al celular del usuario, según este elija en el proceso de establecer la autenticación en dos pasos. También podrá seleccionar si usar la MFA únicamente para acceder a una cuenta desde un nuevo dispositivo o cada cierto tiempo. Algunos servicios permiten la verificación en dos pasos en sus servicios[22].

Generalmente, la MFA combina dos o más credenciales independientes: lo que sabe el usuario (contraseña), lo que tiene el usuario (token de seguridad) y lo que es el usuario (verificación biométrica), como ejemplifica la siguiente tabla:

Algo que sé	Algo que tengo	Algo que soy
Una contraseña: - Un número telefónico - Una fecha de nacimiento - Una dirección - Nombre de alguna mascota	Token de seguridad o contraseña enviada por: - Un SMS - Un mensaje por aplicación - Un correo electrónico	Datos biométricos[23]: - Identificación facial - Identificación de huella dactilar - Otro

Más información en "Todo lo que debes conocer sobre las contraseñas"[24] de INCIBE.

22 Para más información, ver: https://www.google.com/landing/2step/?hl=es_419#tab=how-it-works

23 Son las propiedades físicas, fisiológicas, de comportamiento o rasgos de personalidad. Son atribuibles a una sola persona y son medibles.

24 Para más información, ver: https://www.incibe.es/sites/default/files/contenidos/blog/antes-pyme-con-contrasenas-fuertes-que-sencillas/infografia-contrasenas-para-pymes.png

Anexo 4. Base para protocolo de respuesta ante un incidente

Existen varios tipos de ciberincidentes que pueden presentarse en una institución escolar. La respuesta que debe tenerse ante ellos dependerá de la legislación de cada país, pero el "Esquema Nacional de Seguridad de Gestión de Ciberincidentes"[25] es un referente avanzado que puede tomarse como modelo base para la respuesta.

La respuesta a un ciberincidente comprende varias fases, como muestra esta gráfica:

Ciclo de vida de la Respuesta a Ciberincidentes

1. **La fase de preparación** consiste en instaurar protocolos (anexo 1) y monitoreo (anexo 2).
2. **La fase de detección, análisis e identificación** comienza por clasificar el ciberataque con base en seis criterios principales:

    a. Tipo de ataque[26].
    La peligrosidad de un ataque puede ir de 1 al 5, donde 1 es bajo y cinco es crítico, como se muestra la tabla:

Nivel	Peligrosidad
1	BAJO
2	MEDIO
3	ALTO
4	MUY ALTO
5	CRÍTICO

25 Para más información, ver https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

26 Para conocer más de la clasificación de peligrosidad recomendamos consultar la página 12 del Esquema Nacional de Seguridad de Gestión de Ciberincidentes.

b. Origen de la amenaza.

c. Perfil de los usuarios afectados (es decir, quiénes fueron afectados. Por ejemplo, solo alumnos, docentes, todo el personal, etc.).

d. Número y tipo de los sistemas afectados[27].

e. Impacto y consecuencias posibles.

f. Requerimientos legales y regulatorios (estos dependen de cada país).

3. **La fase de contención, mitigación y recuperación** pueden verse en este anexo y en el anexo 5.

4. **La fase de actividad pos-ciberataque** requiere evaluar el proceso en forma global y generar una bitácora con detalles del incidente, como:

   a. Resumen de las acciones realizadas para la contención del ciberincidente, la erradicación del ciberincidente y la recuperación de los sistemas afectados.

   b. Impacto del ciberincidente, medido en tipología de la información o sistemas afectados, posible interrupción en las clases o cualquier otro servicio escolar, tiempo y costos propios y ajenos hasta la recuperación del funcionamiento normal de las actividades escolares, pérdidas económicas (en caso de que aplique) y daños reputacionales asociados.

Uno de los ciberincidentes que más amenazan la privacidad y seguridad de sus estudiantes es la fuga de datos. Para enfrentar una fuga de datos, además del protocolo para dar una respuesta general a ciberincidentes, debería contarse con un protocolo de prevención de respuesta ante incidentes.

27 Para conocer más sobre la clasificación de los ciberataques recomendamos consultar la página 8 de la Guía de ciberseguridad.

A continuación, se describe cómo podría verse este tipo de protocolo para fugas de datos con base en una Guía del INCIBE[28] (2012).

Fase	Descripción
Fase inicial	• Detección del incidente • Alerta del incidente a nivel interno • Inicio del protocolo determinado por el plantel
Fase de lanzamiento	• Reunión del equipo de crisis designado internamente • Informe inicial de la situación • Coordinación de primeras acciones y establecimiento de la causa de la fuga • Determinación de los siguientes pasos
Fase de valoración	• Valoración inicial del incidente • Elaboración de un informe preliminar
Fase de evaluación	• Reunión del equipo de crisis designado • Presentación del informe preliminar • Determinación de principales acciones • Asignación de tareas y planificación
Fase de contención	• Ejecución de todas las acciones del plan. Puede incluir el establecimiento de canales de comunicación con los afectados por el incidente y localización de los datos (si fueron difundidos públicamente).
Fase de seguimiento y estabilización	• Valoración de los resultados del plan • Gestión de otras consecuencias • Informe completo para compartir con la comunidad educativa, docentes, padres y madres de estudiantes afectados por el incidente • Aplicación de medidas y mejoras • Restablecimiento de la actividad con las nuevas medidas de seguridad

En caso de que los datos afectados se hayan hecho públicos, el INCIBE recomienda:

- Identificar en dónde se hicieron públicos los datos, así como el tipo y cantidad de datos.
- Recopilar las noticias que se hayan hecho al respecto en medios de comunicación.
- Analizar las reacciones que se hayan dado ante el incidente.

28 Para más información, ver: https://www.incibe.es/extfrontinteco/img/File/intecocert/Formacion/EstudiosInformes/guia_gestion_fuga_informacion.pdf

Anexo 5. Base para protocolo de informe sobre incidente a padres y madres

Una vez iniciado el protocolo de acción ante fallas de seguridad de datos de la institución educativa, es importante informar a las personas cuyos datos se hayan visto afectados: estudiantes, padres y madres.

Se recomienda tomar las siguientes acciones (INCIBE, 2012):

- Informar del incidente y especificar qué datos fueron vulnerados. De esta manera se pueden tomar las acciones oportunas como, por ejemplo, cambios de contraseñas, bloqueos de cuentas o lo que corresponda según el caso.
- Establecer un canal de comunicación formal con padres y madres donde puedan responderse todas sus dudas, así como darles recomendaciones y seguimiento acerca del protocolo y avance de la remediación del incidente por parte de la institución educativa.
    - Es importante dar recomendaciones puntuales en caso de que deban seguirse pasos para mitigar las afectaciones que la falla de seguridad pudo originar.
    - Se recomienda que la comunicación se haga por correo electrónico o línea telefónica.
- Comunicar el debido cierre de la brecha de seguridad y las medidas que se seguirán para prevenir futuras fallas de seguridad.
- Revisar los manuales de uso de datos personales en el país donde ocurrió el incidente para ejercer medidas legales en caso de requerirse.

Anexo 6. Protocolo para seleccionar plataforma(s) y herramienta(s) de comunicación adecuadas

De acuerdo con La guía para docentes sobre la privacidad de datos de estudiantes[29] (Connect Safely, 2016) y la Guía sobre la protección de niños y adolescentes contra el uso de tecnologías en las escuelas[30] (Dados Estudiantis), se presentan a continuación algunas preguntas guiadas para evaluar si un servicio tecnológico, ya sea una plataforma, sitio web o aplicación, protege los datos digitales de sus estudiantes. Gran parte de estas preguntas pueden responderse a partir de la lectura de los Términos o condiciones de uso y la Política de privacidad del servicio, por lo que su revisión intencional y a conciencia es de vital importancia para determinar si su uso es adecuado.

Antes de comenzar a utilizar cualquier plataforma con sus estudiantes es importante revisar las opciones de privacidad y seguridad que brinda y personalizar las funciones de acuerdo con el uso escolar que se requiere de ese servicio, de manera que se procure la mayor protección posible.

Preguntas guiadas para evaluación de plataformas

Nota: No todas estas preguntas deben resolverse necesaria y contundentemente en un lapso corto, sino que son una guía para comenzar un mejor manejo de los datos escolares.

- ¿El servicio recolecta información personal estudiantil identificable?
    - » Es importante saber exactamente cómo y qué datos recolecta el servicio.
- ¿El servicio se compromete a no compartir la información estudiantil más allá de lo necesario que requiere el servicio educativo[31]?
    - » Por ejemplo, ¿guarda la información con terceros o vende datos? Este último punto tendría que ser explícito.
    - » Los datos recolectados y utilizados por el servicio deberían estar relacionados con la finalidad y funcionalidad del servicio. Por ejemplo, si la plataforma tiene fines educativos no debe solicitar información sobre datos de salud.
- ¿El servicio crea perfiles de sus estudiantes fuera de los propósitos educativos especificados?
    - » No es recomendable que se creen perfiles fuera de los propósitos autorizados.
    - » De nuevo, los datos recolectados y utilizados por el servicio deben estar relacionados con la finalidad y funcionalidad del servicio.
- ¿El servicio señala quién es responsable de la gestión de los datos almacenados en la empresa proveedora del servicio?

29 Para más información, ver (en inglés): https://www.connectsafely.org/wp-content/uploads/2016/05/Educators-Guide-Data-.pdf

30 Para más información, ver (en portugués): https://www.dadosestudantis.org.br/modulo06.html

31 Es importante evaluar cuáles son los datos que la escuela considera relevantes y cuáles está prohibido recolectar. Este criterio queda en consideración de la institución educativa y debería estar siempre en línea con las regulaciones de cada país.

  - » El controlador u operador es quien se encarga del tratamiento de los datos recopilados, almacenados y usados por un servicio tecnológico y es responsable por un mal uso de los mismos y por violaciones de privacidad.
  - » Siempre que sea una opción posible en el servicio tecnológico en cuestión, es recomendable que la institución educativa sea la responsable designada del tratamiento de los datos.
- ¿Los padres y madres de familia, o bien, la institución educativa, tienen acceso a los datos digitales que recopila y almacena el servicio?
  - » Para poder tener visibilidad sobre los datos que se usan, padres, madres o tutores deberán tener acceso a esos datos.
- Al terminar de usar el servicio, ya sea por cancelar la cuenta o eliminar la aplicación, ¿el servicio elimina todos los datos estudiantiles recolectados y generados?
  - » Es recomendable que los datos recopilados se eliminen una vez que deje de usarse el servicio, así como conocer previamente cuánto tiempo se almacenan los datos.
- ¿El servicio muestra publicidad a los usuarios (estudiantes) en la página web o aplicación usada?
  - » En cuanto a publicidad, se recomienda evitar que los anuncios mostrados sean con base en datos estudiantiles, es decir, que funcione a través de segmentación por comportamiento, pues esto significaría que el servicio rastrea el comportamiento estudiantil en línea y recopila datos más allá de los necesarios para el servicio educativo de interés para la institución escolar.
  - » Es importante fijarse en este punto sobre todo en aquellos servicios que no están diseñados específicamente para ser herramientas educativas.
- ¿El servicio se compromete a proveer seguridad apropiada para los datos que recolecta y almacena?
  - » Se recomienda un servicio que utiliza encriptación al resguardar o transmitir datos. La encriptación de datos es una capa de protección que aumenta el nivel de seguridad.
- ¿El servicio señala que su política de privacidad puede cambiar sin aviso previo?
  - » Una advertencia de esta índole indicaría que no es recomendable su uso en las instituciones educativas, pues en todo momento debe procurarse el consentimiento para la recolección y uso de datos estudiantiles. El cambio repentino de políticas de privacidad en un servicio no permitiría darle el seguimiento adecuado.
- ¿Hay reseñas o artículos acerca del servicio que sean preocupantes?
  - » Es necesario investigar acerca de lo que se ha dicho del servicio antes de usarlo con sus estudiantes.

Anexo 7. Análisis de plataforma(s) y herramienta(s) de comunicación con estudiantes

A continuación, se presenta un análisis de las opciones que ofrecen, en términos de privacidad y seguridad para los datos digitales, diversas plataformas y aplicaciones que suelen utilizarse en el ámbito educativo, sean o no diseñadas específicamente para la educación.

1. Características de seguridad y privacidad que deben revisarse para elegir servicios de videollamadas para clases en línea

Se recomienda asegurarse de que el servicio tenga las siguientes características:

- Seleccionar uno por uno los contactos que quieran añadirse antes de iniciar una videollamada. Por ejemplo, en este video[32], el INCIBE explica cómo usar cierta plataforma en forma segura.
- Escoger si compartir o no información acerca de su actividad en la plataforma.
- Bloquear a usuarios si se percibe algún comportamiento inusual.
- Ajustar los permisos de los diversos canales de comunicación en la plataforma, para que estos se restrinjan a distintos grupos de personas según se seleccionen. Esta opción permite que los mensajes públicos sean únicamente aquellos pertinentes para que todos los estudiantes los vean, y mantener en canales específicos de comunicación aquellos que incumben a estudiantes en particular.
- Seleccionar quién tiene acceso al contenido de documentos compartidos y qué tipo de acceso tiene como, por ejemplo, si puede editar o solo ver.
- Revisar los permisos de las aplicaciones que se agreguen dentro de la plataforma.
- Asignar permisos específicos como anfitrión.
- Poner la función de sala de espera, lo que permite que el anfitrión dé acceso a la reunión únicamente a aquellos participantes que seleccione (ha habido casos en los que se publicaron contraseñas de videoconferencias que eran vulnerables y eso permitió que se unieran personas que no estaban autorizadas).
- Proteger la sala de reunión virtual con contraseña[33] (Zoom, 2020).
- Deshabilitar la opción de compartir pantalla.
- Contar con cifrado de extremo a extremo.
- Activar la función Toc toc, que enseña a los contactos la transmisión de video antes de que contesten la llamada.
- Aceptar o rechazar el enlace[34] de invitación antes de iniciar una conversación con alguien (Protect Young Eyes).
- Controlar si otras personas pueden encontrar por su número de teléfono o por su dirección de correo electrónico a los integrantes de la plataforma.

32 Para más información, ver https://www.youtube.com/watch?v=ys3k1yEPevo&feature=youtu.be

33 Para más información, ver https://blog.zoom.us/es/keep-uninvited-guests-out-of-your-zoom-event/

34 Para más información, ver (en inglés), https://protectyoungeyes.com/apps/google-duo-parental-controls/

Recomendaciones generales para videollamadas

La Agencia Nacional de Seguridad de Estados Unidos (NSA, por sus siglas en inglés) publicó una guía de seguridad para plataformas de videoconferencias[35] donde se incluyen los siguientes criterios claves de evaluación en términos de seguridad y privacidad (Kaspersky, 2020):

- "¿Utiliza el servicio cifrado de extremo a extremo, lo que limita la posibilidad de que otros espíen la llamada?
- ¿Utiliza autenticación de factores múltiples, una opción que protege en forma efectiva las cuentas de los usuarios?
- ¿La tecnología en la que se basa es de código abierto, que puede inspeccionarse, lo que se considera más seguro que el software de propietario, imposible de inspeccionar?
- ¿Comparte la herramienta información con terceros o afiliados?
- ¿Pueden los usuarios borrar de forma segura los datos del servicio y de sus repositorios cuando lo necesiten (tanto el cliente como del lado del servidor)?".

Si bien todas las plataformas de videoconferencia tienen algunas oportunidades de mejora de su seguridad, lo óptimo sería usar aquellas que brinden las mayores medidas de protección adecuadas para el uso de estudiantes. Además, se recomienda acompañar su utilización con buenas prácticas que aumentarán la seguridad y protección de estudiantes y docentes en la plataforma:

- Compartir el enlace con estudiantes unos minutos antes de comenzar la clase en línea por un canal previamente autorizado.
- Evitar compartir el enlace en foros públicos donde podría perder el control de quién lo puede ver y usar.
- Asignar a un responsable desde la institución educativa —el docente, por ejemplo—, que tenga el control de quién accede a la videoconferencia, así como de los permisos para compartir pantalla, utilizar micrófonos y videos.
- Evitar compartir información personal a través de los chats de las salas de videoconferencia.
- Usar la opción de grabar llamada únicamente cuando sea necesario, dado que cada país tiene un protocolo de uso de imagen.
- En caso de grabar, avisar siempre a estudiantes o padres y madres, si corresponde.

35 Para más información, ver https://www.zdnet.com/article/heres-the-nsas-guide-for-choosing-a-safe-text-chat-and-video-conferencing-service/

2. Otras características de seguridad y privacidad de plataformas web y aplicaciones para uso de docentes y estudiantes

Se recomienda asegurarse de que en la plataforma o aplicación se pueda:

- Elegir una verificación o autenticación de dos pasos y métodos alternativos para verificar la identidad al ingresar a la plataforma.
- Personalizar la información que se muestra en el perfil individual.
- Establecer preferencias sobre el historial y anuncios de publicidad a través del apartado *Datos y personalización*.
- Administrar contactos en el menú *Ajustes de Cuenta*, seguido por *Contactos* e *información compartida*, que permite añadir únicamente a contactos seleccionados y, además, bloquear a aquellos que no se reconozcan o tengan un comportamiento inusual en la plataforma.
- Poder, de manera opcional, publicar mensajes públicos o en chat privado, lo que permite gestionar en qué canal compartir determinada información.
- Editar los permisos para acceder, editar, descargar o visualizar cualquiera de los documentos que se compartan con los estudiantes.
    - Los documentos cuentan con historial de edición para que el docente pueda identificar las ediciones y uso que hacen los estudiantes en el documento.
- Garantizar el acceso a la plataforma únicamente para aquellos usuarios que cuentan con permiso.
- Establecer restricciones de permisos a cierta información para estudiantes no designados. Por ejemplo, las calificaciones de cada estudiante solo pueden verse desde su propia cuenta.
- Tener control acerca de qué información se muestra en cada perfil.
- Definir roles dentro de la plataforma acerca de quién tiene permisos específicos para descarga de documentos.
- Establecer que los usuarios que entran a la plataforma se identifiquen a través de la función *forcelogin*[36].

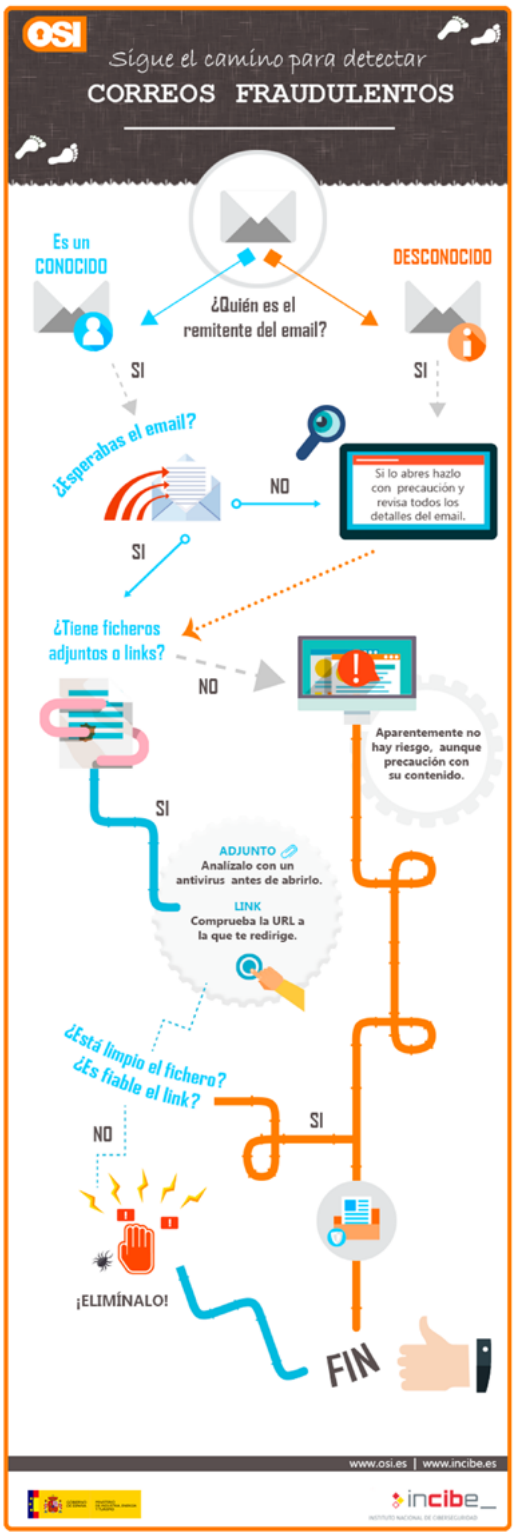
36 En criptografía, un ataque de fuerza bruta consiste en que un atacante envía muchas contraseñas o frases de contraseña con la esperanza de acabar adivinando correctamente una combinación. El atacante comprueba sistemáticamente todas las contraseñas y frases de contraseña posibles hasta encontrar la acertada. De manera alternativa, el atacante puede intentar adivinar la clave que normalmente se crea a partir de la contraseña, utilizando una función de derivación de claves (Fuente: Adleman, Leonard M.; Rothemund, Paul W.K.; Roweis, Sam; Winfree, Erik (June 10–12, 1996). On Applying Molecular Computation to the Data Encryption Standard. *Proceedings of the Second Annual Meeting on DNA Based Computers*. Princeton University).

3. Amenazas al correo electrónico

Para evitar y mitigar las amenazas por correo electrónico lo ideal es que la institución educativa provea una cuenta de correo electrónico de uso estrictamente institucional a su planta de docentes, personal directivo y estudiantes. Al igual que con cualquier plataforma web o aplicación, se recomienda:

- Utilizar una contraseña robusta, cambiarla periódicamente y, en lo posible, una autenticación de dos pasos.
- Incorporar, en lo posible, tecnologías antimalware y verificación de enlaces en el servicio de correo electrónico.

Además, se debe tener precaución con los correos desconocidos que se reciban, pues existen correos fraudulentos y maliciosos que podrían poner en riesgo la seguridad de los datos o contener un virus. La siguiente gráfica provee información para detectar correos fraudulentos (OSI, 2015):



4. Precaución de uso de redes sociales

Como parte de la plantilla educativa de una institución, es preferible no utilizar redes sociales para las actividades en línea con estudiantes, porque son plataformas abiertas a quien quiera entrar y no un sistema cerrado en el que puede controlarse la privacidad y seguridad de los integrantes (en este caso, alumnos). También se recomienda dar la instrucción a los estudiantes de no usar un correo institucional para generar una cuenta en redes sociales, pues podrían rastrear su identidad o el estudiante podría perder el acceso a la cuenta de correo.

Anexo 8. Sugerencias de apartados sobre uso de plataformas digitales para reglamento de la escuela

Algunas secciones sugeridas para añadir al reglamento en cuanto a temas digitales —desde uso de plataformas web y aplicaciones, hasta comportamiento durante las actividades de educación en línea— son estas:

1. Las plataformas web y aplicaciones de uso educativo oficiales en la institución, tales como aquellas para:
    a. Apoyo para las clases.
    b. Videoconferencias.
    c. Comunicación entre docentes y estudiantes; se sugiere, además, establecer un horario para llevarlo a cabo.
    d. Comunicación entre personal directivo, docentes y padres y madres. Se sugiere, además, establecer un horario para hacerlo.

2. Especificaciones acerca de:
    a. Las conductas requeridas durante las clases en línea, tanto de docentes como de estudiantes (por ejemplo: prender la cámara o no).
    b. Los permisos para grabar, fotografiar y compartir la sesión educativa por videoconferencia.
    c. El tipo de plataformas educativas autorizadas para actividades escolares.
    d. La responsabilidad de cada individuo de garantizar que los archivos compartidos no contengan virus.
    e. Las consecuencias de un ciberataque interno (OEA, s.f.).

Anexo 9. Propuesta de carta de notificación para padres y madres (incluye información sobre el tema)

Antes de escribir la carta de notificación es necesario revisar la legislación de protección de datos del país concernido para asegurarse de cumplir los términos y condiciones necesarios.

Debido a que la legislación varía de país a país, es necesario primero consultar los requerimientos nacionales de un aviso de privacidad. Esta carta es solo un ejemplo.

CARTA DE NOTIFICACIÓN DE PADRE, MADRE O TUTOR/A (Gobierno de México)[37]

[CIUDAD Y FECHA]

[PERSONA E INSTITUCIÓN A LA QUE SE DIRIGE]

Por medio de esta comunicación manifiesto que estoy enterado/a acerca de la inclusión de temas digitales en el reglamento de la institución educativa y del protocolo de plataformas web para uso escolar en [NOMBRE DE LA INSTITUCIÓN], así como de la recolección, uso y almacenamiento de datos de mi hijo/a [NOMBRE], de [EDAD] años de edad, quien actualmente estudia en el [NÚMERO DE GRADO] grado escolar, que estas implican.

FIRMA, NOMBRE Y DATOS DE IDENTIFICACIÓN DE PADRE O MADRE

_____
PADRE

_____
MADRE

EN AUSENCIA DE LOS PADRES, NOMBRE Y FIRMA DE QUIEN EJERZA LA PATRIA POTESTAD O TUTORÍA.

_____

37 Para más información, véase: https://www.gob.mx/cms/uploads/attachment/file/453174/Carta-autorizaci_n_Padre-o-tutor.pdf

Anexo 10. Sugerencia de estrategia de comunicación para hablar de privacidad con directores, administrativos, docentes, estudiantes y padres y madres (recursos)

Dentro de las actividades escolares pueden armarse campañas informativas para dar a conocer más sobre el tema de riesgos e importancia de la protección de datos digitales.

1. Personal (directores, administrativos, docentes)

- El entrenamiento en temas de uso ético y responsable de herramientas digitales para la educación, de manera que se asegure la privacidad y seguridad de datos digitales de los estudiantes, necesita idealmente una capacitación al personal directivo, administrativo y docente que requiera usar tecnologías para la educación.

Recursos en línea de utilidad con información pertinente para docentes

- Serie de videos informativos sobre ciberseguridad[38] elaborados por INCIBE. Incluye videos cortos e interactivos en el contexto escolar, de utilidad para formación en el tema.
- Kit de concienciación sobre ciberseguridad[39] creado por INCIBE. Incluye materiales gráficos, lecturas, presentaciones con información de las mismas y un test de evaluación.

2. Estudiantes

Recursos en línea de utilidad para uso escolar con estudiantes:

Los siguientes recursos son actividades de apoyo para conscientización del tema que pueden realizarse en el salón de clases entre docente y estudiantes:

- Taller para docentes y estudiantes sobre "datos inteligentes"[40]. Incluye la presentación de una serie de actividades sencillas para llevar a cabo con los estudiantes y una guía para docentes sobre cómo utilizar la presentación.
- Actividad que fomenta el aprendizaje de pautas sencillas de ciberseguridad[41] en plataformas educativas online. Incluye un cuestionario que puede responderse en la página web.

38 Para más información, ver https://itinerarios.incibe.es/

39 Para más información, ver https://www.incibe.es/protege-tu-empresa/blog/actualizate-ciberseguridad-el-nuevo-kit-concienciacion

40 Para más información, ver https://en.datasmartkids.com/recursos

41 Para más información, ver https://www.is4k.es/educadores/test-plataformas-educativas-online

3. Padres, madres y tutores

- La transición digital de las clases ha visibilizado la importancia de la labor de padres y madres en el seguimiento del aprendizaje de niñas y niños en línea (UNICEF, 2020), subrayando la necesidad de extender la campaña comunicativa o proporcionar sesiones informativas acerca de la protección de datos digitales de los estudiantes.
- Es recomendable que la institución educativa establezca las vías de comunicación apropiadas entre el personal directivo y docentes con los padres y madres para hacerles llegar informes del tema, recursos o invitaciones a sesiones informativas (si es posible realizarlas).

Recursos en línea de utilidad con información pertinente para padres y madres:

- Herramientas de apoyo e información dirigida a padres y madres[42] para la sensibilización acerca del tema, en el portal de Internet Segura For Kids.

42 Para más información, ver https://www.is4k.es/de-utilidad/recursos/material-de-difusion-para-centros-educativos

Anexo 11. Puntos para compartir en una campaña de información

En una campaña de información pueden compartirse aspectos como los siguientes:

- Importancia de proteger los datos digitales.
  - » Derecho de niñas y niños a la privacidad e importancia del consentimiento.
- Riesgos de privacidad y seguridad que vulneran los datos digitales y sus consecuencias:
  - » Ciberataque / hackeo.
  - » Fuga de datos.
  - » Rastreo de actividad en línea.
  - » Venta de datos.
- Medidas de seguridad en dispositivos:
  - » Cortafuegos.
  - » Antivirus.
- Importancia de llevar a cabo prácticas para una mayor protección de los datos de niños y niñas:
  - » Creación de contraseñas robustas.
  - » Lectura de términos y políticas de privacidad en las plataformas web y aplicaciones antes de comenzar a utilizarlas.
  - » Configuración de privacidad, de acuerdo con su uso.
  - » Realización de prácticas cíclicas.

Glosario[43]

- **Antivirus**: programa que ayuda a proteger los dispositivos contra la mayoría de los virus, gusanos, troyanos y otros tipos de malware que pueden infectar los dispositivos.
- **Ciberataque**: conjunto de acciones ofensivas contra sistemas de información como bases de datos, redes computacionales, etc., hechas para dañar, alterar o destruir instituciones, personas o empresas.
- **Cifrado de extremo a extremo**: en las comunicaciones (chats, por ejemplo), se refiere a que los mensajes están seguros y que solo el remitente y el receptor pueden leer el contenido.
- **Cookies**: fichero que guarda nuestro navegador, donde se almacenan pequeñas cantidades de datos que usan los servidores de las páginas webs que visitamos para guardar distintos tipos de información que nos identifican al volver a visitarlas.
- **Copia de seguridad**: herramienta destinada al almacenamiento de datos o información con el fin de disponer de un medio para recuperarlos en caso de pérdida accidental o intencionada.
- **Datos personales:** información de cualquier tipo que pueda ser usada para identificar, contactar o localizar a una persona.
- **Malware**: software diseñado intencionalmente para causar daños a un computador, servidor, cliente o red informática.
- **Sistema operativo**: software que coordina y dirige todos los servicios y aplicaciones que utiliza el usuario en un computador.

43 El glosario está basado en la Guía de ciberseguridad de la Secretaría de Telecomunicaciones (Gobierno de México, 2020).

Fuentes consultadas y referencias

Arias Ortiz, Elena y Julián Cristia. (2014). El BID y la tecnología para mejorar el aprendizaje: ¿Cómo promover programas efectivos? Washington, DC: Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/El-BID-y-la-tecnología-para-mejorar-el-aprendizaje-¿Cómo-promover-programas-efectivos.pdf

Bojalil, Paulina y Carlos Vela-Treviño. (2019). Despuntan las reformas en materia de protección de datos en América Latina. BID: febrero 12. https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/

Cibersecurity & Infrastructure Security Agency. (2021). Ransomware reference materials for K-12 school and school district IT staff. US Government. https://www.cisa.gov/ransomware-reference-materials-k-12-school-and-school-district-it-staff

Comunicaciones. (2020). Guía de ciberseguridad para el uso de redes y dispositivos de telecomunicaciones. México: Secretaría de Comunicaciones y Transportes. https://drive.google.com/file/d/13z_PWUQvycbLTzVMAWbKjfTO4l6l2ZRX/view

Conejo Valley Unified School District. (s.f.) https://www.conejousd.org

Contreras, Belisario (coord.). (2020). Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe. Washington, DC: BID y OEA. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

ESET. (2017). Eset Security Report Latinoamérica 2017. https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

González, Yolanda (2020). Control parental y seguridad de los menores en Internet. Madrid: Grupo Ático 34. Junio 4. https://protecciondatos-lopd.com/empresas/control-parental/#Por_que_es_tan_importante_controlar_el_contenido_que_ven_nuestros_hijos_en_internet

Instituto Nacional de Bioseguridad. (2012). Gestión de fuga informática. España: Ministerio de Industria, Energía y Turismo. León (España): INCIBE. https://www.incibe.es/extfrontinteco/img/File/intecocert/Formacion/EstudiosInformes/guia_gestion_fuga_informacion.pdf

Instituto Nacional de Bioseguridad. (2016). Guía de almacenamiento seguro de la información. León (España): INCIBE. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_almacenamiento_seguro_metad_0.pdf

Instituto Nacional de Bioseguridad. (2017). Dispositivos móviles personales para uso profesional (BYOD). Una guía de aproximación para el empresario. León (España): INCIBE. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_dispositivos_moviles_metad.pdf

Instituto Ponemon, IBM. (2020) Cost of a Data Breach Report 2020. USA: IBM. https://www.ibm.com/security/data-breach

Kaspersky (2020) Cyber Security Risks: Best Practices for Working from Home and Remotely. https://www.kaspersky.com/resource-center/threats/remote-working-how-to-stay-safe

OECD. (1999). Online Advertising and Marketing Directed Toward Children. OECD Digital Economy Papers, No. 46. Paris: OECD Publishing. https://www.oecd-ilibrary.org/science-and-technology/online-advertising-and-marketing-directed-toward-children_236506677507;jsessionid=uI9s3Ad_5jvO3P3PVgII_uIU.ip-10-240-5-52

Oficina de Seguridad del Internauta. (2013). Creando contraseñas robustas. Diciembre 5. https://www.osi.es/es/actualidad/blog/2013/12/05/creando-contrasenas-robustas

Organización de Estados Americanos. (s.f.). Reglamento de uso del aula virtual. portal.oas.org/LinkClick.aspx?fileticket=nCougUTRFpk=&tabid=1905

Organization of American States. (2020). Educación en ciberseguridad. Planificación del futuro mediante el desarrollo de la fuerza laboral. Washington: OEA. www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf

Saigal, Rahul. (2020). Does Your Mac Really Need a Firewall? What You Need to Know. MUO. February 25. https://www.makeuseof.com/tag/mac-really-need-firewall/

The London School of Economics and Political Science. (2020). My data and privacy online. A toolkit for young people. London: LSE. https://www.lse.ac.uk/my-privacy-uk/for-educators

UNESCO. (2017). International Symposium on School Violence and Bullying: from Evidence to Action. Seoul: UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000246970

UNICEF. (2020). Mamás y papás deben apoyar el aprendizaje de las y los adolescentes en el hogar. Bolivia: UNICEF. https://www.unicef.org/bolivia/historias/mamás-y-papás-deben-apoyar-el-aprendizaje-de-las-y-los-adolescentes-en-el-hogar

UNICEF. (2019). COVID-19: Preparación y respuesta educativa. Respuesta de UNICEF a los desafíos de educación en América Latina y el Caribe durante el COVID-19. Panamá: Unicef. https://www.unicef.org/lac/en/covid-19-education-preparedness-and-response

United Nations. (2020). Policy Brief. Education during COVID-19 and beyond. New York: UN. https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2020/08/sg_policy_brief_covid-19_and_education_august_2020.pdf


eon
resilience lab
by C Minds


BID
Mejorando vidas