

Aprendizaje en línea seguro

Políticas y gobernanza para la protección
de datos de los estudiantes en América
Latina

Claudia May Del Pozo
Ana Victoria Martín del Campo Alcocer
Mariana Róo Rubí

Sector Social
División de Educación

DOCUMENTO PARA
DISCUSIÓN N°
IDB-DP-00894

Aprendizaje en línea seguro

Políticas y gobernanza para la protección de datos de los estudiantes en América Latina



Aprendizaje en línea seguro

Políticas y gobernanza 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**, **Cristina Martínez Pinto**, **Mariana Róo Rubí**, **Daniela Rojas** y **Carla Vázquez Wallach** (C Minds); **Cristina Pombo** y **Natalia González Alarcón** (BID Sector Social); **Elena Arias** (BID Sector Educación) y **Santiago Paz** (BID Ciberseguridad).

Septiembre 2021

<https://www.iadb.org/>

Copyright © 2021 Banco Interamericano de Desarrollo. Esta obra se encuentra sujeta a una licencia Creative Commons IGO 3.0 Reconocimiento-NoComercial-SinObrasDerivadas (CC-IGO 3.0 BY-NC-ND) (<https://creativecommons.org/licenses/by-nc-nd/3.0/igo/legalcode>) y puede ser reproducida para cualquier uso no-comercial otorgando el reconocimiento respectivo al BID. No se permiten obras derivadas.

Cualquier disputa relacionada con el uso de las obras del BID que no pueda resolverse amistosamente se someterá a arbitraje de conformidad con las reglas de la CNUDMI (UNCITRAL). El uso del nombre del BID para cualquier fin distinto al reconocimiento respectivo y el uso del logotipo del BID no están autorizados por esta licencia CC-IGO y requieren un acuerdo de licencia adicional.

Note que el enlace URL incluye términos y condiciones adicionales de esta licencia.

Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan el punto de vista del Banco Interamericano de Desarrollo, de su Directorio Ejecutivo ni de los países que representa.



Tabla de contenido

Agradecimientos

Por su generosidad de tiempo y 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 Cruz, Directora de Recursos Tecnológicos en Capa8, Escuelas Ciberseguras (México); **Carla Vázquez Wallach**, Especialista en derecho digital, Fundadora de Legal + Innovation e integrante del *Brain Hive* de C Minds (México); **Cristina Martínez Pinto**, Fundadora y Directora del spinout de C Minds, PIT Policy Lab, y Consultora de Política Pública en C Minds (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 agradecimiento y reconocimiento a las personas entrevistadas durante la investigación, pues sus perspectivas fueron claves para enriquecer el documento:

Alejandro Morduchowicz, Especialista Líder en Educación en la División Educación del BID (regional); **Andrew Young**, Director de Conocimiento de The GovLab (Estados Unidos); **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 Directora del Departamento de Recursos Tecnológicos del 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**, Presidente del Plan Ceibal (Uruguay) y Especialista Líder en Educación en la División Educación del BID (regional); **Montserrat Creamer**, Especialista de Educación en Ecuador (Ecuador); **Priscila Gonsales**, Directora Nacional de Educadigital (Brasil), y **Víctor Giorgi**, Director General de Instituto Interamericano del Niño, la Niña y Adolescentes del Organismo de los Estados Americanos (OEA) (regional).

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

Anedia Taño Núñez (México), **Carola Betzabé Huaranga Ospino** (Perú), **Enrique Castañeda Zúñiga** (Perú), **Gabriela Pagliaso** (Argentina), **Gloria Elizabeth Galeano Álvarez** (Paraguay), **Graciela Pozzer** (Argentina), **Iris Peña** (Panamá), **Marcela Róo Cancino** (México), **Marian Núñez Núñez** (México), **Patricia Santanaria Guaminí** (Ecuador), **Roberto Antonio Carmona Caro** (Colombia) y **Silvia Medina** (Argentina).

Por último, un especial agradecimiento a nuestros socios de difusión de la Encuesta de Escuelas en Línea Seguras LATAM, por sumarse con tanto entusiasmo a la iniciativa:

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

Prefacio

Acerca del BID

Banco Interamericano de Desarrollo (BID) - Sector Social

El Sector Social (SCL) está conformado por un equipo multidisciplinario que actúa bajo la convicción de que la inversión en las personas permite mejorar sus vidas y superar los desafíos del desarrollo en América Latina y el Caribe. Junto con los países de la región, el Sector Social formula soluciones de política pública para reducir la pobreza y mejorar la prestación de servicios de educación, trabajo, protección social y salud. El objetivo es construir una región más productiva donde predomine la igualdad de oportunidades para hombres y mujeres, y una mayor inclusión de los grupos más vulnerables

Banco Interamericano de Desarrollo (BID) - Sector Educación

El Sector Educativo es un sector transdisciplinario que apoya a los países de América Latina y el Caribe a promover la enseñanza efectiva y el aprendizaje de todos los niños y jóvenes de la región. A su vez, promueve el desarrollo de habilidades y el aprendizaje permanente como estrategia para lograr que los ciudadanos puedan hacer una contribución productiva a la sociedad, incrementar su bienestar y ser buenos ciudadanos.

Este informe hace parte de la iniciativa fAIr LAC del BID

fAIr LAC responde a los esfuerzos del BID por construir un entendimiento común de lo que es la IA, sus oportunidades y sus aplicaciones, pero también sus riesgos y las posibles medidas para mitigarlos. En colaboración con socios y aliados estratégicos, esta iniciativa co-desarrollada con C Minds busca promover la adopción responsable de la IA para mejorar la prestación de servicios del Estado (principalmente en los sectores de educación, salud, protección social, mercados laborales y temas asociados con género y diversidad) y crear oportunidades de desarrollo en aras de reducir las brechas y atenuar la creciente desigualdad social. [https://www.iadb.org/es/fAIr LAC](https://www.iadb.org/es/fAIr-LAC)

Prólogo BID

Desde antes de la pandemia, los niños, niñas y jóvenes de la región están expuestos al uso de la tecnología más que ninguna otra generación. [En el 2018](#), en promedio, 6 de cada 10 estudiantes de América Latina contaban con acceso a un computador para realizar las tareas de la escuela en sus hogares. En Uruguay y Chile, 8 de cada 10 estudiantes reportaron acceso a un computador en sus hogares. Sin embargo, aunque cada vez más estudiantes en la región tienen acceso a dispositivos y a internet, estas cifras esconden grandes brechas entre grupos de estudiantes favorecidos y vulnerables, dado que en promedio solo 3 de cada 10 estudiantes de bajos ingresos cuentan con este acceso.

La pandemia ha acelerado esta tendencia, aumentando la exposición de niños y jóvenes a la tecnología y a los contenidos digitales: fueron las únicas herramientas para mantener alguna continuidad educativa. En efecto, 165 millones de niños y jóvenes en América Latina y el Caribe (ALC) dejaron de asistir a la escuela y perdieron en promedio de 158 días de aprendizaje presencial durante el 2020. Hoy, a más de un año del comienzo de la pandemia, y pese a que varios países de la región han comenzado una reapertura gradual de los centros educativos, muy pocos países se encuentran con sus escuelas completamente abiertas.

En este contexto, los gobiernos de la región han apostado por poner en marcha modelos de educación híbridos para hacer frente al cierre de los centros educativos. Sin embargo, la doble emergencia sanitaria y educativa, los puso al frente de nuevos retos para los cuales las escuelas no estaban preparadas: el control de acceso, la integridad de los datos y la protección del contenido para mantener sus cursos y sus estudiantes seguros. Los problemas de seguridad en internet han ido creciendo en todos los sectores, y educación no se queda atrás. Los hackers han empezado a aprovechar las vulnerabilidades de los sistemas escolares, por lo que se ha observado un aumento progresivo de la gravedad de los ataques.

El año pasado, en Estados Unidos, más de 500 escuelas fueron atacadas con *ransomware*, y los hackers exigieron \$ 1,6 millones de dólares. Pero esto no pasa solo en Estados Unidos. En agosto del 2020, la página web del Ministerio de Educación de Panamá (Meduca) recibió ataques cibernéticos y los estudiantes perdieron acceso a las clases en línea. En Chile y en [Colombia](#), distintas universidades también han sido el blanco de ataques cibernéticos. Y así podemos encontrar ejemplos en casi todos los países de la región.

Las escuelas cuentan con planes para las diversas emergencias que pueden surgir: desde desastres naturales como terremotos o huracanes, hasta accidentes como incendios e incluso para la eventualidad de robo o tiradores activos. ¿Por qué el abordaje de la ciberseguridad en la escuela debería ser distinta? El desafío no es el uso de la tecnología en sí, sino la falta de marcos normativos y gobernanza apropiada en los distintos niveles del sistema educativo para asegurar que se cuenta con regulaciones claras en cuanto a la recolección, almacenamiento, acceso y uso de los datos de los menores.

Debemos apoyar a la comunidad educativa, directores de escuela, maestros, familias y adultos a cargo de niñas, niños y jóvenes a desarrollar planes y protocolos que permitan generar entornos seguros y aprovechar al máximo la tecnología para la educación.

El objetivo de este estudio es justamente generar conciencia en la comunidad educativa de los países de la región sobre la importancia de impulsar una gobernanza de datos de sistemas educativos centrada en los derechos de los estudiantes. Para ello hemos consultado directamente a la comunidad educativa a través de encuestas, adelantado una revisión de regulación y normativa vigente, y realizado entrevistas a expertos y expertas de la región. Adicionalmente, el estudio busca documentar iniciativas y procedimientos que nos ayuden a establecer protocolos sobre la manera más efectiva de recopilar, almacenar, utilizar y distribuir datos sensibles e información personal de estudiantes y docentes.

Los resultados muestran que la mayoría de los países de la región no ha conseguido hasta la fecha proporcionar a maestros y estudiantes herramientas que garanticen un uso seguro de la tecnología y de la educación híbrida y a distancia, sin poner en riesgo los datos y la privacidad de los y las estudiantes.

Desde el BID estamos apoyando a los países en la implementación de una hoja de ruta para preparar a los educadores, fortaleciendo el aprendizaje híbrido y a distancia, al tiempo que promovemos un entorno seguro y una utilización responsable de la tecnología. Como parte de nuestra Visión 2025, trabajaremos para asegurar que las iniciativas de capital humano estén alineadas con nuestros esfuerzos en salud, igualdad de género, transformación digital y acción climática para promover una recuperación verde y equitativa. Es imperativo y responsabilidad de todos y todas proteger la privacidad y seguridad de nuestros niños y niñas y velar porque el uso de estas plataformas no exponga sus datos a un uso indebido.

La tecnología es fundamental para la educación en momentos de distanciamiento social, y su importancia sólo seguirá creciendo en el futuro. Esperamos que las lecciones de este documento sean una referencia útil y que, en definitiva, contribuyan a lograr un aprendizaje en línea seguro para todas y todos.

Mercedes Mateo,
Jefa División de Educación del BID

Acerca de C Minds + Eon Resilience Lab

C Minds es una organización mexicana liderada por mujeres que busca fomentar la igualdad de oportunidades para facilitar vidas más plenas a través del aprovechamiento de nuevas tecnologías como la inteligencia artificial (IA). La organización se especializa en diseñar e implementar estrategias para el cambio social en países emergentes en respuesta a los nuevos paradigmas desencadenados por la transformación tecnológica masiva. C Minds trabaja con gobiernos, organizaciones multilaterales e instituciones locales implementando proyectos con los que se busca incrementar la resiliencia de las comunidades, preparar a las diferentes industrias para el futuro, proteger el medio ambiente y promover un desarrollo de las nuevas tecnologías centrado en los derechos humanos. www.cminds.co

El Eon Resilience Lab (ERL) de C Minds tiene por misión preparar a individuos para enfrentar un futuro incierto y digital a través de colaboraciones con actores clave de todos los sectores, privado, gobierno y organismos multilaterales, buscando una transformación digital inclusiva. Promueve diálogos entre actores en la intersección de temas prioritarios y nuevas tecnologías y lleva a cabo proyectos pilotos para explorar los límites y las oportunidades que nos ofrecen éstas mismas en México y América Latina.

Prólogo Eon

El Eon Resilience Lab cree firmemente que la tecnología puede usarse como herramienta clave para adaptarse con éxito a las situaciones adversas e inesperadas que se presentan cada vez con más frecuencia. Bajo esta convicción, nuestra misión es trabajar bajo un esquema colaborativo con los gobiernos, la academia, la industria, las organizaciones multilaterales y otros actores de cambio en el diseño de estrategias dirigidas a fortalecer las capacidades institucionales de América Latina y el Caribe desde perspectivas panorámicas.

El proyecto de protección de datos de la niñez nació al explorar las oportunidades y los riesgos del uso de sistemas de IA para los niños y las niñas, en particular en temas de educación. Al indagar esta temática, nos percatamos que primero había un reto clave previo al uso de tecnologías disruptivas. Esta realidad reorientó nuestro trabajo para investigar la privacidad, seguridad y protección de los datos de menores en instituciones educativas y, con base en estos aprendizajes, crear recomendaciones para una óptima digitalización de la educación.

Nos enorgullece ser socios del Grupo BID en esta tarea crucial de fortalecer a la región en el uso responsable de tecnología para beneficio de la educación. Esperamos que este informe ayude a visualizar con claridad los avances de Latinoamérica en este campo y a su vez contribuya a promover las conversaciones y acciones necesarias para el aprovechamiento ético de la tecnología en ámbitos escolares, así impulsando una región más próspera, justa e inclusiva. Esto dependerá en buena medida de nuestra capacidad de profundizar las preguntas y encontrar respuestas de manera colectiva.

Claudia Del Pozo,

Directora del Eon Resilience Lab de C Minds

Resumen ejecutivo

Desde principios de 2020 y hasta la fecha de publicación de este reporte, algunas de las escuelas donde estudian más de 168 millones de niños y niñas del mundo llevan más de un año entero cerradas debido a la pandemia del Covid-19 ([UNICEF](#), 2021). Como respuesta de emergencia, a raíz de la pandemia, millones de estudiantes, docentes y directores tuvieron que migrar de manera masiva a plataformas digitales para no interrumpir su aprendizaje y enseñanza.

Una de las lecciones de esta pandemia son las ventajas y oportunidades educativas que traen las tecnologías en la educación, señalando una probable alza constante en su adopción en el futuro. Como lo menciona el BID, “el uso de tecnología será una herramienta para la continuidad pedagógica” (Álvarez Marinelli, et al., 2020), lo que significa que cada vez más alumnos se conectarán para tomar clases en línea, creando una huella digital exponencial de datos de menores de edad.

Aún cuando el uso de la tecnología es fundamental para la educación en momentos de distanciamiento social, y su importancia sólo seguirá creciendo en el futuro, el uso de estas plataformas pone a los niños y las niñas en un estado de vulnerabilidad si los datos que se recolectan y guardan de ellos y ellas no son gestionados de manera que protejan su privacidad y seguridad. A su vez, y de la misma manera que las escuelas resguardaban la información privada de sus estudiantes en cajones con llave, es importante transferir este cuidado al mundo digital, asegurando la privacidad, protección y seguridad de los dispositivos de almacenamiento o de acceso a datos digitales. Nos enfrentamos a un reto nuevo en el sentido que la transición masiva de operaciones y personas a plataformas en línea causada por la pandemia se realizó de forma apresurada, sin considerar, en muchas ocasiones, lo que podría significar que estas tecnologías registraran todos los aspectos de la experiencia educativa de estudiantes menores de edad y ciertos aspectos de su vida personal, en ocasiones, ampliando o generando una huella digital a temprana edad.

Si bien la privacidad, protección y seguridad de datos se presentan en conjunto, en este reporte estos tres conceptos se refieren a conceptos se refieren a distintos aspectos de salvaguardar datos. La seguridad son los límites de acceso que se pactan entre los dueños y quienes recolectan, almacenan y resguardan los datos; la protección refiere al respeto de la finalidad de uso que se le da a los datos y la seguridad refiere a la robustez técnica de la infraestructura y los sistemas que recolectan, almacenan y tratan los datos. Una administración pública de datos completa (gobernanza) debería cumplir con estos tres conceptos.

Para que esto suceda, se deben atender varios retos en la región: por un lado, retos estructurales que limitan la conectividad de estos estudiantes y, por otro lado, retos de conocimiento, que no permiten que los alumnos sepan aprovechar dicha conectividad para su educación. Las directrices que ofrecen consejos, guías y principios para ayudar a los niños y las niñas a utilizar los servicios en línea de forma más segura son valiosas y un primer paso en la implementación de protección en escuelas, pero los problemas estructurales de gobernanza de datos requieren soluciones específicas para la educación desde sus ministerios y secretarías, no soluciones únicamente para los individuos, además del marco de acción que brindan las legislaciones de privacidad. En este sentido, un análisis

de la regulación y normas existentes en Latinoamérica en materia de privacidad de datos destacó una latente necesidad de impulsar políticas y normas específicas para que las distintas instituciones de gobierno puedan tener una administración de datos de estudiantes responsable, ética y que atienda a los riesgos de privacidad, protección y seguridad que surgen del uso de tecnologías en el ámbito educativo.

Es importante que los países de Latinoamérica impulsen una gobernanza de datos de sistemas educativos centrada en los derechos de los estudiantes. Esta gobernanza requeriría un conjunto de iniciativas y procedimientos que prescriban la manera correcta de recopilar, mantener, utilizar y distribuir los datos sensibles, concretamente la información personal de estudiantes y docentes. Este reporte busca servir de insumo para que las Secretarías y Ministerios de Educación de la región sigan desarrollando políticas, procedimientos y responsabilidades que proporcionen claridad en torno a los datos de los estudiantes y del distrito en cada etapa de su ciclo de vida, preparando el camino para que la información proteja los derechos de privacidad, confidencialidad y seguridad del estudiante o de los individuos, como lo han hecho desde antaño.

El reporte reúne insumos de (1) Entrevistas semi-estructuradas individuales con 15 personas expertas¹ en distintas temáticas relacionadas al proyecto, (2) Dos conversatorios regionales con docentes de cuatro países (3) Un equipo de 7 personas expertas que conforman el Consejo Asesor² y (4) La Encuesta de Aprendizaje Seguro en Línea LATAM en la que participaron 1,300 docentes y directivos de instituciones educativas de seis países³, la primera de su tipo y generada para los fines de este reporte. Con base en el análisis holístico del estado actual de la privacidad, protección y seguridad de datos en Latinoamérica y los insumos de los ejercicios anteriores, se generaron las siguientes recomendaciones para la protección de datos de los estudiantes en ámbitos educativos, que se pueden encontrar con más detalle en el el reporte. A continuación se comparte un resumen de las recomendaciones junto con los actores a las que van orientadas en paréntesis:



I. Promover una estructura organizacional y gobernanza de datos a través del desarrollo de marcos normativos y regulatorios

1. Reformar la legislación para actualizarla a las necesidades de protección, seguridad y privacidad de datos de la niñez, comenzando por ámbitos educativos (Autoridad de Educación y/o de Datos o Datos personales)
2. Crear reglamentos y normas para la recolección y uso de datos (Autoridad de Educación y/o de Datos)
3. Crear grupos de trabajo interinstitucionales para tomar los primeros pasos hacia la creación de una Autoridad de Datos, si es que el país no tiene (Gobierno)
4. Explorar los beneficios y riesgos de la IA y otras nuevas tecnologías basadas en el uso masivo de datos (Autoridad de Educación y/o de Datos, Academia, Sociedad Civil)

1 Los nombres de estas personas expertas temáticas, de nueve países de América se encuentran en la página 2, en la sección de Agradecimientos, de este reporte.

2 Los nombres de las personas expertas del Consejo Asesor, de 4 países distintos, se encuentran en la página 2, en la sección de Agradecimientos, de este reporte.

3 Los seis países son: Brasil, Costa Rica, Colombia, México, Perú y Uruguay



II. Fomentar el desarrollo de capacidades

1. Promover la educación y campañas de concientización en el tema a todos los niveles (Autoridad de Educación y/o de Datos o Sociedad Civil)
2. Facilitar cursos para una navegación segura en línea diferenciados por perfiles (Autoridad de Educación y/o de Datos o Sociedad Civil)
3. Desarrollar un directorio de expertos y expertas en temas relevantes para la protección de datos digitales de menores en ámbitos escolares y materia de privacidad, ética, datos, plataformas digitales educativas (Autoridad de Educación y/o de Datos, Academia y/o Sociedad Civil)
4. Fortalecer la comunidad de práctica educativa latinoamericana (Autoridad de Educación y/o de Datos y/o Sociedad Civil)



III. Invertir en infraestructura tecnológica para la aplicación de la norma

1. Invertir en la infraestructura necesaria para que servidores y proveedores públicos y privados puedan cumplir con las normas y marcos de protección, privacidad y seguridad de datos.
2. Establecer estándares para que en cualquier proceso de contratación pública se respeten los lineamientos y estándares de protección, privacidad y seguridad de datos.
3. Establecer protocolos de seguridad en ambientes educativos (Autoridad de Educación y/o de Datos)



IV. Fomentar políticas complementarias en temas de conectividad, brecha digital e inclusión

1. Fortalecer la conectividad del país e invertir en la calidad de ésta para fines educativos (Autoridad de Telecomunicación y de Educación)
2. Analizar a profundidad los impactos de la brecha digital en el entorno educativo, en contexto del Covid-19 (Gobierno, Academia y/o Sociedad Civil)
3. Desarrollar estrategias de inclusión focalizadas a grupos y comunidades marginadas y vulnerables como suelen ser los pueblos indígenas. (Autoridades de Educación e Instituciones y Organismos de Inclusión).

Metodología

Con el objeto de hacer un diagnóstico del estado y de las necesidades, así como de los retos y oportunidades alrededor de la protección de datos digitales de los estudiantes en ámbitos escolares de Latinoamérica, además de la investigación documental se llevaron a cabo tres actividades en el marco del proyecto **Aprendizaje Seguro en Línea**: (1) Entrevistas semiestructuradas individuales con 15 personas expertas, (2) Dos conversatorios regionales con docentes de cuatro países y (3) La Encuesta de Aprendizaje Seguro en Línea LATAM, en la que participaron 1300 personas de seis países.

(1) Entrevistas individuales con personas expertas

Las entrevistas se realizaron en forma de video virtual con 15 actores destacados de gobierno, academia, industria y sociedad civil, con un enfoque en temas de creación de capacidades para los sectores público y privado, necesidad de infraestructura técnica para lograr la seguridad de los datos escolares, mecanismos de supervisión y monitoreo así como colaboraciones intersectoriales y multisectoriales para el fortalecimiento del ecosistema.

Estas entrevistas semiestructuradas permitieron profundizar en los retos y las oportunidades que enfrenta la región, con énfasis en cada país y sector, lo cual sirvió como insumo para el desarrollo de recomendaciones puntuales de política pública modificada para adaptarse a diferentes contextos. Para conocer a las personas entrevistadas, puede referirse a la sección de agradecimientos de este reporte.

(2) Conversatorios regionales con docentes

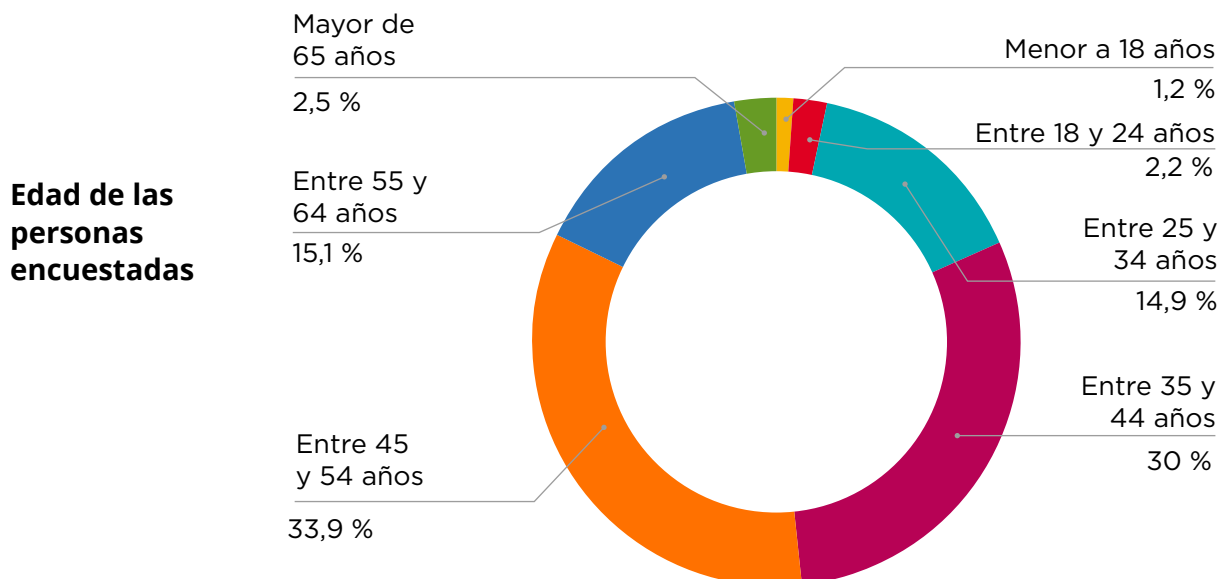
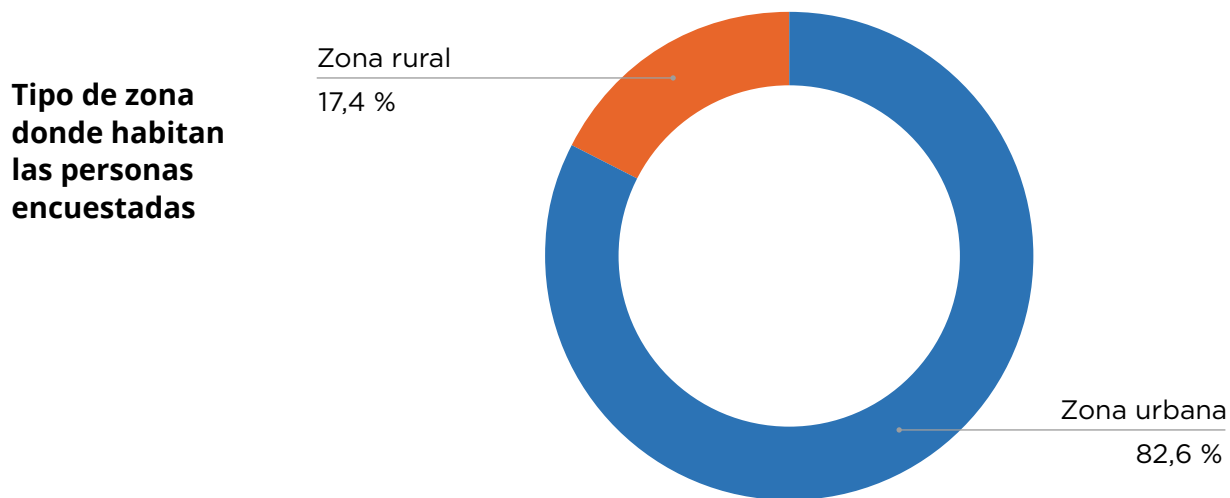
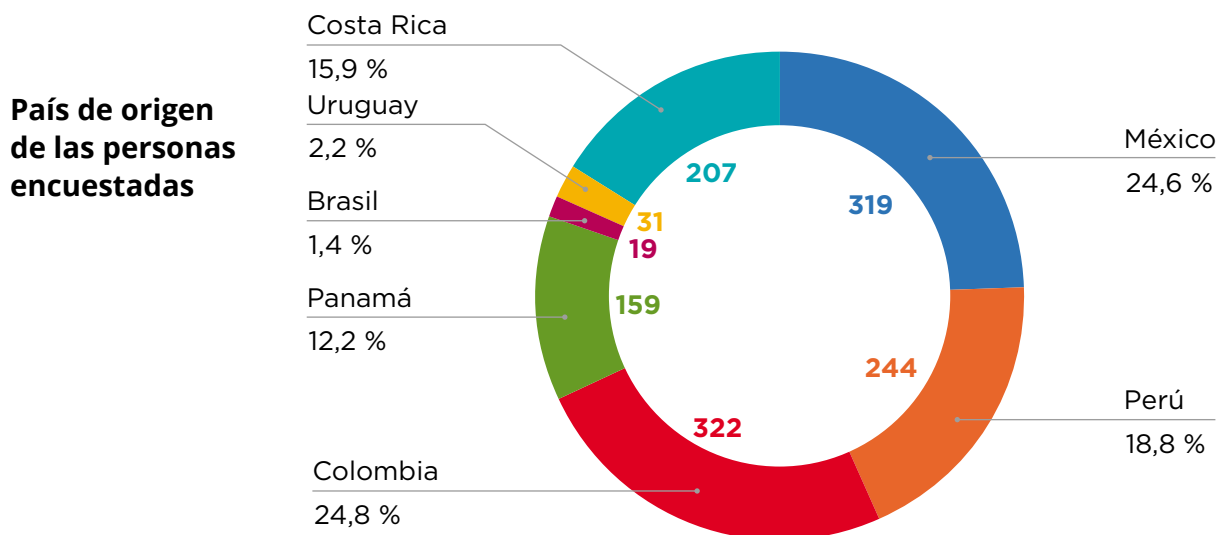
Se realizaron dos conversatorios regionales con docentes de Argentina, Ecuador, México y Perú. Su objetivo fue conocer diversas perspectivas sobre los retos que enfrentan o enfrentaron en la transición digital, sus experiencias y preocupaciones para tomarlas en cuenta en este reporte. Las personas que participaron en los conversatorios aparecen en la sección de agradecimientos.

(3) Encuesta de Aprendizaje Seguro en Línea LATAM

Con el objetivo de entender, en forma anónima, el nivel de concientización de docentes y directores sobre el tema de privacidad de datos de niños y niñas en ámbitos escolares y así complementar la información desde la perspectiva de los beneficiarios, como parte del proyecto se realizó una **Encuesta de Aprendizaje Seguro en Línea LATAM sobre la perspectiva de docentes y directores de instituciones educativas acerca de la protección de datos de los estudiantes**. La contestaron aproximadamente 1300 docentes de seis países de Latinoamérica, con lo que se logró crear conocimiento nuevo a través de la única encuesta de su tipo en la región.

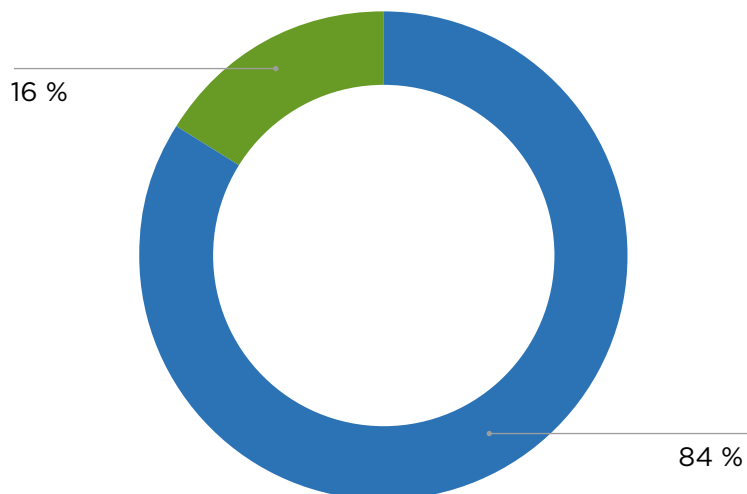
Respuestas de la Encuesta de Aprendizaje Seguro en Línea LATAM:

Número final: Contamos con **1301** respuestas finales.



Ocupación de las personas encuestadas

- Docente, profesor titular, asistente de profesor, profesor de materia extracurricular
- Directivo

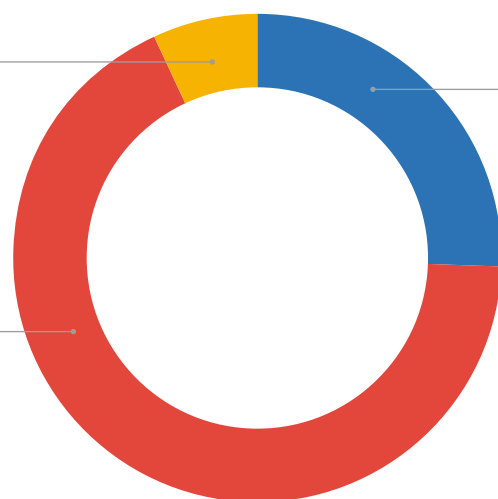


Tipo de institución educativa a la que pertenecen las personas encuestadas

Otro tipo
de institución
6,7 %

Privada
25,6 %

Pública
67,7 %



Grado escolar con la que trabajan las personas encuestadas

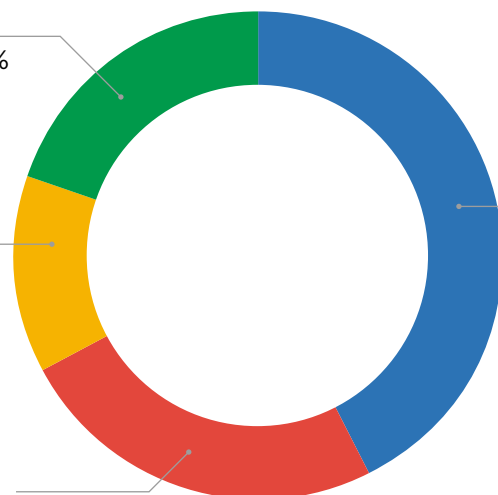
- **Educación primaria** (primeros 6 grados de escolaridad), educación general básica primaria
- **Educación secundaria alta** (grados 9-12), educación media, educación general media Ciclo 2, bachillerato, educación secundaria del 4^{to} al 5^{to} grado (9-12 años de escolaridad)
- **Educación secundaria baja** (grados 6-9), educación secundaria del 1er al 3er grado, ciclo básico de educación media (6-9 años de escolaridad)
- **Educación media** con énfasis en educación para el trabajo (años 9-12 + año 13 de escolaridad si aplica)

19,6 %

13,1 %

24,6 %

42,7 %



1. Introducción

“Evitar que una crisis de educación se vuelva una catástrofe generacional requiere la actuación urgente de todos.”- [UNICEF](#), 2020

Desde principios de 2020 y hasta la fecha de publicación de este reporte, las escuelas donde estudian más de 168 millones de niños del mundo llevan más de un año entero cerradas debido a la pandemia del Covid-19 ([UNICEF](#), 2021). Como respuesta de emergencia, a raíz de la pandemia millones de estudiantes, docentes y directores tuvieron que migrar de manera masiva a plataformas digitales para no interrumpir su aprendizaje y enseñanza. Hasta entonces, las escuelas habían empezado la adopción de procesos y herramientas digitales, pero la pandemia hizo que este avance –visto como opcional– se volviera un requisito indispensable para poder ofrecerle continuidad a uno de los fundamentos más básicos de la sociedad: la educación.

Esta transición masiva de operaciones y personas a plataformas en línea se realizó en forma apresurada, sin considerar, en muchas ocasiones, lo que podría significar que estas plataformas se apoderaran de todos los aspectos de la experiencia educativa de estudiantes menores de edad y ciertos aspectos de su vida personal. Además, en ocasiones ampliando o en algunos casos generando huella digital desde muy jóvenes o niños.

Si bien ya existía una nueva generación “datificada” desde temprana edad ([Young](#), 2020), la institución escolar está contribuyendo a este proceso al permitir la recolección de datos demográficos e información relacionada con la programación, la asistencia, la disciplina, la salud, la elegibilidad para los programas escolares, las calificaciones, los resultados de los exámenes y los programas académicos, entre otros, así como los datos creados o generados por estudiantes o docentes al usar plataformas educativas.

Es importante mencionar que los datos de menores de edad se consideran sensibles⁴ o hasta altamente sensibles⁵ ([Martínez](#), s.f.) en los países de la Organización de Estados Americanos (OEA). Aun cuando el uso de la tecnología es fundamental para la educación en momentos de distanciamiento social y su importancia seguirá creciendo en el futuro, el uso de estas plataformas pone a niños y niñas en un estado de vulnerabilidad si sus datos, que se recolectan y guardan, no se gestionan de manera que protejan su privacidad y seguridad.

4 Los datos sensibles son “datos personales que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, o membresía sindical (...), datos genéticos, datos biométricos con el propósito de identificar de manera única a una persona física, datos relacionados con la salud o datos relativos a la vida sexual u orientación sexual de la persona [traducción propia].” Processing of special categories of personal data (Reglamento General de Protección de Datos GDPR, 2018), Artículo 9. <https://gdpr-info.eu/art-9-gdpr/>

5 En algunos países, los datos altamente sensibles tienen regulaciones específicas y en algunos casos incluso se prohíbe su tratamiento.

Por eso mismo, es fundamental transferir el cuidado de la privacidad y seguridad que tenían de la información de sus estudiantes en el mundo físico al mundo digital. Ante esta necesidad apremiante es prioritario que, desde los gobiernos, con un enfoque principal en los Ministerios y Secretarías de Educación, puedan atenderse los retos y se creen mecanismos de apoyo y directrices para las instituciones educativas. Asimismo, es necesario que se guíe el desarrollo, la adopción de procesos y plataformas digitales, se promueva entre los actores clave un mayor entendimiento de los riesgos asociados y se desarrollen estrategias para su mitigación ([Gamito et al., 2016](#)), pues se están exponiendo la institución educativa, su personal y los estudiantes en el ambiente escolar.

Dado que el uso masivo de plataformas digitales es incipiente en los ámbitos educativos de la mayoría de los países latinoamericanos, no existe un consenso sobre los derechos digitales de niños y niñas, ni regulaciones para proteger su privacidad, específicamente en plataformas escolares y procesos digitales de las instituciones educativas. El contexto actual es un momento no solo óptimo, sino también crucial para que instancias gubernamentales líderes en la materia, como los Ministerios y Secretarías de Educación y entidades de manejo de información, puedan sentar las bases para el manejo de datos de niños y jóvenes en ámbitos educativos.

Por esta razón, el [Grupo BID](#) y el [Laboratorio de Resiliencia Eón](#) de [C Minds](#), por iniciativa [fAlr LAC](#)⁶ del BID, se han aliado para diseñar e implementar el proyecto de **Aprendizaje Seguro en Línea**. Tras la publicación de una guía del BID y C Minds para la protección de datos escolares para docentes, el proyecto presenta este **Reporte de recomendaciones sobre políticas y gobernanza para la protección de datos de los estudiantes en América Latina**.

Este documento busca acelerar el entendimiento y diálogo sobre los retos y visibilizar buenas prácticas de varios países, además de proveer recomendaciones de política pública para fortalecer la protección de datos digitales de los niños en ámbitos educativos desde la administración pública en Latinoamérica (principalmente enfocado a Ministerios y Secretarías de Educación). Asimismo, el reporte pretende que autoridades nacionales de protección de datos, legisladores, organizaciones de la sociedad civil, instituciones especializadas en educación de los sectores público y privado, asociaciones escolares de padres y madres de familia y otros actores que juegan un rol dentro del ciclo de aprendizaje puedan beneficiarse de las recomendaciones suministradas, las cuales buscan señalar que existen oportunidades diversas para atender desde los sectores público y privado los desafíos mencionados.

Alcance del reporte

El reporte no pretende ser exhaustivo ni prescriptivo. Si bien el tema del impacto de la digitalización y de las nuevas tecnologías en la vida de los niños es muy amplio, el alcance de este reporte se centra en el ámbito educativo. Considerando que la navegación en plataformas educativas solo representa una parte de la actividad de ellos en línea, se ofrece una Recuadro informativa con ejemplos puntuales de otras temáticas tangenciales igual de relevantes en torno a la protección de datos, pero sin ahondar en estas.

6 fAlr 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. Para más información, véase <https://fairlac.iadb.org/es>

El objetivo de estos ejemplos es ofrecerle al lector información general de otros temas que hay que considerar para atender en forma integral el desafío de la datificación de los menores de edad. Es importante reconocer que si bien el ámbito educativo es un enfoque clave para la protección de datos de niños y niñas, no es el único que deben discutir y atender los actores de interés. Finalmente, las temáticas de datos, así como de tecnología, evolucionan con rapidez, por lo cual es necesario actualizarse constantemente.

2. Contexto

La pandemia del Covid-19 impactó en todas las áreas de la vida de las personas: desde el ámbito social, al profesional y al educativo. Según la Organización de las Naciones Unidas (ONU) “la pandemia del Covid-19 ha generado la disrupción más grande en la historia de los sistemas educativos, afectando a 1.6 miles de millones de estudiantes en más de 190 países y en todos los continentes” ([ONU](#), 2020). En cuestión de semanas, a inicios de 2020, más de 168 millones de niñas y niños en todo el mundo se encontraron en un esquema de distanciamiento social, sin posibilidad de ir a su escuela o colegio.

En el momento de publicación de este reporte en muchos casos se cumple más de un año de esta situación. Para evitar que la pandemia impactara la educación de toda una generación, la mayoría de las instituciones educativas optó por implementar rápidamente, sin mucho criterio de análisis de riesgos e implicaciones, nuevos mecanismos de aprendizaje y enseñanza a través del uso de plataformas digitales o tecnologías de la información (TIC). Si bien esta solución ofreció beneficios que eran impensables en el pasado (por ejemplo, en la pandemia de Estados Unidos de 1918 o del virus de la gripe A H1N1, gran parte del alumnado no tuvo otra opción que seguir yendo a la institución educativa a pesar de los riesgos de salud ([Waldrop](#), 2020)), esta digitalización apresurada trajo consigo una serie de retos, en particular para garantizar la seguridad y privacidad de datos digitales tanto de estudiantes como de docentes.

2.1 Beneficios de las soluciones digitales y de las nuevas tecnologías

Según un reporte de [UNICEF](#) (2021), en la mayoría de las investigaciones examinadas para ese reporte sobre el impacto de la tecnología en la educación se ha señalado que el aprendizaje potenciado por la tecnología ha facilitado la adquisición de conocimientos y habilidades. Una de las áreas críticas en las que la tecnología ha mejorado la comprensión es el pensamiento crítico, pues los estudiantes están capacitados para abordar y aprovechar las oportunidades. Además, la digitalización les ha permitido entrar en una era de aprendizaje digital, encabezada por la adopción de las TIC para apoyar a las instituciones educativas a tomar decisiones más informadas. Gracias a ello, parece que el aprendizaje se ha vuelto más personalizado en los programas de educación complementarios a las clases presenciales, aprovechando los datos generados por cada estudiante.

Recuadro 1. Ejemplo de plataforma educativa lanzada por el sector público
([Gómez Mont et al.](#), 2020).

El Plan Ceibal es el Plan de Conectividad Educativa de Informática Básica para el Aprendizaje en Línea, del gobierno de Uruguay. Este proyecto socioeducativo digital incluye el programa Plataforma Adaptativa de Matemática (PAM), que es una plataforma adaptativa en línea que complementa la enseñanza de matemáticas de los docentes con procesos educativos personalizados, según las necesidades de cada estudiante. Asimismo, brinda a los maestros herramientas para trabajar con sus grupos, establecer metas de aprendizaje y proponer actividades. Cuenta con instrumentos de evaluación integral para hacer seguimiento y elaborar informes en forma inmediata, que utilizan sistemas de IA para asesorar a los maestros y personalizar el avance educativo.

Debido al confinamiento establecido como medida de salubridad pública a nivel global en la pandemia del Covid-19, de acuerdo con el Banco Mundial, no solo fue el sector salud, sino también el sector educativo, el que tuvo que responder de manera rápida y eficaz a los nuevos retos en más de 120 países, adoptando e incorporando tecnología a sus dinámicas para no interrumpir la educación básica, media y superior ([Cobo et al.](#), 2020).

En forma general, las respuestas más ágiles ante la imposibilidad de continuar las clases presenciales fueron aquellas que se desarrollaron desde gobiernos que tenían cierto nivel de preparación para un ámbito educativo digital, al igual que por parte de gobiernos que reaccionaron con rapidez y ofrecieron una solución integral, como fue el caso del gobierno de Costa Rica que presenta el Recuadro 2.

Recuadro 2. Implementación de la plataforma educativa ministerial de emergencia de Costa Rica ([BID](#), 2020).

En cuestión de meses, el gobierno de Costa Rica, desde el Departamento de Recursos Tecnológicos, habilitó correos electrónicos a más de un millón de estudiantes. En colaboración con el Instituto Costarricense de Electricidad (ICE) se abrió una línea telefónica de apoyo técnico para docentes y estudiantes. También se habilitó el acceso a la plataforma de una empresa experta en computación para promover la conexión entre docentes y se activaron datos telefónicos gratuitos para su uso.

Para que el acceso a la página fuera seguro y los datos de los estudiantes que ingresaran no se vieran comprometidos en las plataformas digitales, el gobierno brindó formación a más de 30.000 docentes (50 % del total a nivel nacional) para el uso de dicha plataforma.

Este caso es relativamente único entre los diferentes esfuerzos en la región para garantizar continuidad en la educación, porque toma en cuenta un tema central que muchas otras soluciones dejaron por fuera: la privacidad y seguridad de la información, particularmente de los datos de niños y niñas. Estos dos temas constituyen dos nuevos retos que enfrentan los estudiantes en ámbitos educativos digitales.

Es necesario que cualquier solución que busque ser exitosa y sustentable explore el impacto que podría tener el manejo de la información a modo de riesgos en la vida de las personas posiblemente afectadas, incluyendo a los menores de edad.

A continuación, se explora este tema, poco presente en las conversaciones actuales en torno a la transformación digital educativa.

2.2 La Inteligencia Artificial y su futuro en la educación

Además de los beneficios tecnológicos generales de la tecnología, la Inteligencia Artificial (IA) promete cambiar el panorama educativo para docentes, directores y alumnos dentro de los siguientes 10 años.

La IA⁷ es una tecnología que trae muchas promesas en cuanto a la resolución de desafíos del mundo moderno, pero al mismo tiempo existe cierta conciencia sobre los riesgos que podría desencadenar. Esta tensión se está viviendo en todas las industrias y áreas de la vida cotidiana, incluso en la educación, en la que se espera que esta tecnología pueda impulsar transformaciones educativas importantes. La reducción de la brecha de acceso, la automatización de la gestión, la optimización de los procesos de enseñanza y aprendizaje, la personalización del aprendizaje, la realización de tareas rutinarias de los docentes y el análisis de datos en el ámbito de los sistemas escolares son tan solo algunos beneficios que podría aportar la IA a la educación ([BID, 2020](#)).

Se ha demostrado que las herramientas de aprendizaje con IA ayudan a niñas y niños a desarrollar habilidades como la colaboración, el pensamiento crítico y la resolución de problemas ([ONU, s.f.](#)). El Recuadro 3 presenta tres casos de uso latinoamericano de la IA para el sector educativo.

7 A partir de aquí estaremos refiriéndonos a la sub-rama de la IA llamada Aprendizaje Automático de Máquina (Machine Learning), definida como "programas computacionales que, en lugar de detallar el conjunto de reglas y criterios que un computador debe seguir para cumplir un objetivo, se enfocan en aprender y resolver el problema por sí mismos a partir de datos y ejemplos preexistentes" (BID, 2020).

Recuadro 3. IA para la educación en Latinoamérica

- En Chile se desarrolló un sistema de IA entrenado con datos públicos sobre el contexto educativo, social y geográfico de los estudiantes, capaz de predecir la deserción escolar. Ello le permitió a los actores indicados tomar medidas para reducir este riesgo (BID, 2020b).
- En 2016, en Uruguay se inició un proyecto para crear un sistema nacional de analítica del aprendizaje para monitorear y procesar los datos educativos disponibles en el país. Uruguay es el país de la región que más digitalizado tiene su sistema escolar. La información nueva, obtenida a través del sistema, permitirá adaptar las prácticas de enseñanza, lo que mejorará los desempeños escolares y disminuirá la deserción (BID, 2020b).
- Desde 2013, Uruguay ofrece acceso a la Plataforma Adaptativa de Matemática (PAM) a todos los estudiantes y docentes de Educación Primaria y a los que toman Matemática en Educación Media. Esta plataforma utiliza IA para completar los aprendizajes de los estudiantes en Matemática al ofrecerles apoyo personalizado (fAIR LAC, 2021).

Si bien las instituciones educativas han ido incorporando de forma gradual los sistemas inteligentes para apoyar el trabajo de directivos y docentes, todavía falta explorar los retos que podría implicar para los estudiantes, en particular en cuanto a privacidad de datos⁸. En efecto, los sistemas de IA funcionan al entrenarlos con grandes volúmenes de datos y en el caso del sector educativo se requiere utilizar la información de los estudiantes y sus familias que en su mayor parte se halla disponible en las instituciones escolares.

Según la Encuesta de Aprendizaje Seguro en Línea LATAM, tan solo 6 % de las personas encuestadas afirmaron tener protocolos en caso de filtración de datos escolares, mientras que al menos 48 % indicó no saber si existían estas herramientas. El reto estriba en que no siempre existe conciencia del personal de la escuela o colegio sobre el uso de los datos de manera adecuada en función de los fines específica y explícitamente informados.. Por esta razón es clave que las instituciones escolares alcancen un entendimiento claro sobre el uso que puede darle a los datos, así como los protocolos de seguridad para el cuidado de la información recolectada como por ejemplo la de los estudiantes y sus familias, así como de los integrantes de la administración educativa.

A su vez, no se trata únicamente de fortalecer los procesos de las instituciones educativas para proteger los datos estudiantiles; también se vuelve clave crear marcos de gobernanza eficientes en cuanto a recolección, uso, almacenamiento y acceso a los datos de sus estudiantes. Como lo mencionó el experto de gobernanza de datos Andrew Young, de GovLab, durante su entrevista para este reporte: “los datos grupales y la IA afectan a niños y niñas de una manera única y debe ser entendida de esta manera para poder crear marcos de gobernanza”.

8 Para más información sobre los usos y efectos de la IA en educación, véase: <https://publications.iadb.org/publications/spanish/document/Usos-y-efectos-de-la-inteligencia-artificial-en-educacion.pdf>

Dados los riesgos inherentes que existen para todos los niños en el uso de sistemas de IA, varias organizaciones se han dado a la tarea de crear marcos y lineamientos para el uso de sistemas de IA para que no los afecten a ellos.

Recuadro 4. Ejemplos de marcos existentes para el uso de IA para niños y niñas

- [Principios de Beijing](#) para la Inteligencia Artificial.
- [UNICEF](#) tiene un proyecto que creará investigación para la normativa de IA y los menores de edad.
- El [IEEE](#) cuenta con un estándar para sistema inteligente de seguridad infantil mediante aprendizaje automático en dispositivos IoT (Internet of Things).
- A su vez, la [Comisión Europea](#) dispone de un marco normativo de la IA y un nuevo plan coordinado con los Estados miembros que abordará la seguridad y los derechos fundamentales de las personas y las empresas, al tiempo que reforzará la adopción de la IA en Europa.

Más allá de los riesgos relativamente claros que presentan la falta de privacidad y de seguridad en torno a los datos digitales de los estudiantes, el uso de la IA implica retos más complejos, como el que se presenta en torno al uso ético de sus datos.

Recuadro 5. Ejemplo de un caso de uso de datos digitales de estudiantes en contexto de pandemia

En Alemania, como solución a la imposibilidad de llevar a cabo exámenes para los estudiantes por causa de la pandemia, una universidad decidió predecir las notas que tendría cada alumno a través de un sistema de IA desarrollado por un tercero. El modelo se entrenó con datos que incluían las calificaciones pasadas de cada individuo, así como antiguas calificaciones obtenidas por otros estudiantes. A su vez, estas calificaciones predichas y no reales (pues no reflejaban la capacidad real de cada alumno) sirvieron para determinar su ingreso a la educación superior y el tipo de beca al que tendrían acceso.

Este caso es preocupante, pues se le quitó a los estudiantes la capacidad de influir en su propio futuro, dejándolo en manos de un sistema de IA, y llevó a protestas por parte de la comunidad estudiantil. Además de lo alarmante de la situación, se debe plantear la pregunta sobre qué tan bien calibrado y confiable era el sistema ([Simonite](#), 2020).

2.3 Privacidad, protección y seguridad de datos

Si bien la privacidad, protección y seguridad de los datos se presentan en conjunto, estos tres conceptos se refieren a distintos aspectos de la salvaguardia de datos.

La privacidad se refiere a los límites de acceso que se pactan entre los dueños de los datos y quienes los recolectan, almacenan y resguardan; la protección alude al respeto de la finalidad de uso que se le da a los datos, y la seguridad tiene que ver con la robustez técnica de la infraestructura y los sistemas que recolectan, almacenan y tratan los datos.

En el contexto escolar, la **privacidad de los datos** se encuentra estrechamente vinculado con la intimidad de los estudiantes, familiares y los administrativos de las instituciones educativas, es un derecho garantizado en diferentes instrumentos internacionales y nacionales de derechos humanos⁹.

La **protección de la privacidad** implica que los datos personales únicamente pueden ser tratados para fines legítimos y por medios legales. Concretamente, las preocupaciones prácticas sobre la protección de la privacidad de los datos suelen girar en torno a qué datos se tratan, la finalidad de su procesamiento y cómo se comparten; si los datos se comparten con terceros o cómo se comparten, y cómo estos se recopilan o en su caso se almacenan temporalmente¹⁰.

Por su parte, la **protección de los datos** se enfoca en que los fines del tratamiento de los datos deben ser específicos y una institución educativa o empresa debería indicarlos explícitamente a estudiantes, docentes, padres y tutores al momento de su recolección. A su vez, una organización no podría establecer fines indefinidos, la recolección debe ser limitada ("limitación de la finalidad") y con el conocimiento o el consentimiento del titular ("principio de consentimiento"). Normalmente el aspecto de legalidad se cumple al comunicar por qué es necesario la recolección de los datos o en su caso la normativa sobre la cual descansa la solicitud de información

La organización debe recoger y procesar solo los datos personales que sean necesarios para cumplir con propósitos escolares y educativos ("minimización de datos") y por medios legales, es decir, a través de mecanismos que resultan compatibles con la normativa, finalidad, así como con las expectativas del titular en función de la relación que sostiene con la institución educativa (por ejemplo la organización no podría utilizar la información recolectada para ofrecer y comercializar servicios ajenos a los propósitos previamente comunicados a los titulares).

9 Artículo 5 - Derecho a la protección a la honra, la reputación personal y la vida privada y familiar. Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar. Conferencia Internacional Americana, "Declaración americana de los derechos y deberes del hombre", 1948.

Artículo 11. Protección de la Honra y de la Dignidad. 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques. Convención americana sobre derechos humanos suscrita en la conferencia especializada interamericana sobre derechos humanos, 1969.

10 Esto aparece en diversas restricciones normativas, como el GDPR, la HIPAA, la GLBA o la CCPA.

Los datos personales solamente deben ser recopilados con el conocimiento y consentimiento de los estudiantes, docentes, padres y/o tutores (“transparencia y consentimiento”). La institución educativa proporcionará información clara y suficiente para que el titular tome una decisión (explícito o implícito) para proporcionar sus datos, debe evitarse cualquier duda o ambigüedad al respecto. El mecanismo para obtener el consentimiento debe ser apropiado a la edad y la capacidad de los titulares, así como de acuerdo con las circunstancias particulares del caso y características de los datos.

La institución educativa no puede utilizar los datos personales de sus estudiantes para otros fines que sean incompatibles con la finalidad original que la organización pactó con los distintos miembros de la comunidad educativa ni compartirlos con terceros que no sean aquellos para los cuales se otorgó el consentimiento, excepto en virtud de solicitud de autoridad competente conforme a disposición legal. De igual modo, debería garantizarse que los datos personales no se almacenen durante más tiempo del necesario para los fines para los que fueron recolectados (“limitación del almacenamiento”).

Por último, la **seguridad de datos** implica que la empresa/organización debe instalar las salvaguardias técnicas, administrativas y organizativas razonables y adecuadas que garanticen la seguridad de los datos personales, incluida la protección contra el tratamiento no autorizado o ilegal y contra la pérdida, destrucción o daño accidentales, utilizando la tecnología apropiada. Las instituciones educativas deben ejercer un juicio razonado y fundamentado sobre las medidas preventivas para reducir riesgos, así como para dar respuesta a vulnerabilidades como por ejemplo informar a los titulares sobre accesos no autorizados, pérdida o destrucción de la información.

La seguridad en el entorno digital no debe entenderse como algo estático, las amenazas a la privacidad han ido evolucionando conforme al avance tecnológico por ello deberán considerarse mecanismos constantemente actualizados para evitar obsolescencia. La robustez de las medidas de seguridad dependerá de las características de los datos, por ejemplo, el manejo de datos sensibles requerirá un nivel más alto de seguridad y protección.

Es recomendable que las instituciones educativas implementen mecanismos de monitoreo y evaluación periódicos para mantener medidas eficaces y controles adecuados apropiadas al tratamiento de los datos que realizan.

Como se observa en la siguiente tabla ejemplificativa, una misma acción puede presentar los tres tipos de riesgo. Si bien muchas veces estos riesgos se superponen y un riesgo protección de los datos casi siempre también es de privacidad, es preciso distinguirlos para asegurarse de cubrir bien estas tres necesidades.

Ejemplo de riesgo	Riesgo de protección	Riesgo de seguridad
Utilizar datos estudiantiles para fines no autorizados.	✓	✗
Secuestro (<i>ransomware</i> ¹¹) de hardware o software donde se almacenan o tratan datos personales a los cuales no se puede acceder, pero que se amenaza destruir o divulgar.	✗	✓
Bloqueo de acceso a un software.	✗	✓
Robo de identidad de un estudiante.	✓	✗
Filtración de los datos de una institución educativa por una mala conexión del software a internet o por una debilidad de la página web.	✓	✓
Destrucción del servidor físico donde estaban almacenados los datos.	✗	✓
Aceptación de los miembros de una comunidad para compartir datos con una organización, pero esta no especifica con qué finalidad se usarán.	✓	✗
Presencia de un <i>bug</i> en un sistema, que no permite a los estudiantes acceder a sus cuentas.	✗	✓

2.4 Riesgos de privacidad, protección y seguridad de datos

Aunque la privacidad de los datos¹² siempre ha sido relevante, el alcance de su protección ha crecido en las últimas décadas a medida que se comparte más información en línea, generando cada vez más datos. **A su vez, y de la misma manera que las instituciones escolares resguardaban la información privada de sus estudiantes en archivadores con llave, es importante transferir este cuidado al mundo digital, asegurando la privacidad, protección y seguridad de los dispositivos de almacenamiento o de acceso a datos digitales.**

En un entorno físico, colegios y escuelas se encuentran obligados a proteger los datos personales y la privacidad de todos aquellos de quienes manejen información (personal administrativo y directivo, docentes, tutores, padres de familia y estudiantes). Sin embargo, los riesgos a los que nos enfrentamos en línea son también de protección y seguridad, no solo de privacidad. Si bien esto es cierto desde los inicios de la digitalización de las operaciones de las instituciones educativas, la acelerada transformación digital causada por la pandemia ha generado aún más datos y ha aumentado de manera exponencial el número de ciberataques desde el inicio de la pandemia a principios de 2020 ([UNPRI, 2020](#)). Esta realidad reafirma la importancia de tener redes e infraestructura capaces de resguardar la información de manera segura. El mundo educativo se ha visto afectado en

¹¹ Véase una definición en el anexo 2.

¹² La privacidad de los datos se relaciona con la forma como debe manejarse una información o datos en función de su importancia relativa.

forma particular por esta realidad con la masiva transición hacia las clases en línea, donde **“los ciberdelincuentes ven al sector educativo como un objetivo porque las instituciones educativas guardan datos personales valiosos”** ([Hernández, 2020](#)).

Tan solo en 2018, cuando todavía no había una migración masiva a un Sistema de Información y Gestión Educativa (SIGED)¹³, 67 % de escuelas y colegios de Latinoamérica había sido víctima de ciberataques¹⁴ ([Ortega, 2018](#)). En línea con esta cifra, la **Encuesta de Aprendizaje Seguro en Línea LATAM** revela que 88,6 % de los docentes percibe que ha sido nula o poca la importancia otorgada a la mitigación de riesgos en línea y la privacidad de estudiantes y docentes. A pesar de esta realidad, hasta 94,2 % de las personas encuestadas respondió que no existe o no conoce si su institución educativa cuenta con algún tipo de protocolo para enfrentar este tipo de situaciones. Tan solo 5,7 % reporta contar con un protocolo en caso de violación o filtración de datos.

Esto puede llevar a situaciones de alto riesgo como las que presenta el siguiente Recuadro:

Recuadro 6. Riesgos de un uso de la tecnología relativo a peligros de ciberseguridad

- En marzo de 2021 se suspendieron las clases en línea por más de una semana en Nottinghamshire, ciudad del Reino Unido, por un ciberataque ([Skelton, 2021](#)). Los gobiernos federal y distrital se encargaron de monitorear las consecuencias de este ciberataque y de reforzar las medidas de seguridad. Aunque no hay indicios de que fueron violados los datos personales del personal o de los estudiantes, el insuceso recuerda la importancia de contar con una cultura cibernética¹⁵ para evitar poner en riesgo los datos digitales de estudiantes y docentes.
- En enero de 2021 el gobierno de Inglaterra repartió equipo de cómputo a niñas y niños como medida de apoyo para la continuación de sus estudios en línea, sin saber que ya contenían malware¹⁶ ([Wakefield, 2021](#)). Este malware instala software espía que puede recoger información sobre los hábitos de navegación, así como recopilar información personal, como datos bancarios, por ejemplo, y distribuirlos a terceros no autorizados.

Estas filtraciones de información ponen datos sensibles o altamente sensibles¹⁷ en manos de personas con intenciones dudosas. A continuación, se aclara el tipo de datos digitales que resguarda una institución escolar, así como los riesgos a los que se exponen los estudiantes y docentes si no se cuidan en forma adecuada.

13 De acuerdo con el BID (Arias Ortiz et al., 2021) un sistema SIGED “se puede definir como el conjunto de procesos de gestión educativa que sirven para diseñar, registrar, explotar, generar y diseminar información estratégica en línea de forma integral, enmarcados por una infraestructura legal, institucional y tecnológica concreta.”

14 Véase el anexo 2 para la definición de ciberataque.

15 De acuerdo con IEEE (2003) la higiene cibernética es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, especialmente la información contenida en una computadora o que circula a través de las redes de computadoras.

16 Se puede encontrar una definición en el anexo 2.

17 Como se menciona en la introducción, dependiendo de la regulación de cada país, los datos altamente sensibles, o especialmente protegidos, son una categoría de datos que debido a su incidencia especial en la intimidad, las libertades públicas y los derechos fundamentales de la persona hacen necesaria una mayor protección que en el resto de datos personales.

Tipos de datos que resguarda una institución educativa

Entre los datos que podría recolectar una plataforma educativa están: metadatos de la tecnología de aplicaciones¹⁸, datos de evaluación, trabajos de los estudiantes, pertenencia al programa del estudiante, identificadores de estudiantes, datos curriculares específicos y datos demográficos (para conocer más sobre la clasificación de datos, ir al [anexo 1](#)).

Aquí es importante hacer una distinción según el supuesto en el que se encuentre cada plantel educativo:

1. Este controla el funcionamiento de la plataforma y, por tanto, establece criterios sobre el tratamiento de los datos.
2. Este contrata plataformas de terceros que tienen establecidas reglas sobre el tratamiento.

En ambos casos, escuelas y colegios son responsables del tratamiento, pero deberían conscientizarse sobre las condiciones mínimas que deberían exigir en caso de contratar plataformas externas.

Riesgos de datos digitales en ámbitos educativos

Según UNICEF ([Stoilova, et al., 2020](#)) niños y niñas enfrentan numerosos tipos de riesgo en línea, desde consecuencias para la salud mental, hasta riesgos de ciberseguridad y privacidad. Entre ellos se destacan los siete tipos más comunes de riesgos de *bullying* y violencia que pueden enfrentar los estudiantes en línea: ciberacoso, amenazas por correo electrónico, *flaming*, *outing*, *phishing*, acoso por externos y robo de identidad (para conocer las definiciones, ir al [anexo 2](#)).

Una filtración en una institución educativa podría poner la información personal de los estudiantes en manos equivocadas, afectando la ciberseguridad y hasta la seguridad física de las diferentes personas representadas por los datos que permitirían a perpetradores cometer diversas acciones dañinas.

Además, es importante tener en mente que algunas escuelas o colegios en la región ya manejan datos biométricos¹⁹ de sus estudiantes al utilizar tecnologías de vigilancia o monitoreo, como cámaras, o algunas herramientas digitales que pueden identificar instancias de trampa en exámenes a través de la cámara y el micrófono de la computadora²⁰, por mencionar algunos. Una persona malintencionada podría atacar el sistema de cámaras de la institución educativa, observar las ocurrencias y/o robar datos altamente sensibles

18 La [CEPAL](#) (2020) lo define como el conjunto de información que describe los datos generados, los cuales pueden ser procesados mediante computadoras (CEPAL. 2020. Gestión de datos de investigación. Biblioguías). Véase <https://biblioguias.cepal.org/gestion-de-datos-de-investigacion/metadatos> “

19 Para conocer más acerca de la clasificación y definición de datos biométricos, véase el anexo 1.

20 Estas nuevas herramientas digitales se conectan a las cámaras de la computadora para supervisar los movimientos de los ojos y la cabeza, a micrófonos para registrar el ruido en la sala, y utilizan algoritmos para registrar la frecuencia con la que la persona que está tomando un examen mueve el ratón, se desplaza hacia arriba y hacia abajo en una página y pulsa las teclas. El software señala cualquier comportamiento que su algoritmo considere sospechoso para que el instructor de la clase pueda revisarlo. (Feathers, 2020)

de reconocimiento facial. También podría aprovechar directamente las herramientas que usa la cámara de la computadora para observar a un estudiante en particular, sin su conocimiento²¹. De acuerdo con regulaciones actuales a lo largo de la región latinoamericana, usualmente los datos biométricos solo pueden recolectarse si existe una normativa que así lo permita o, bien, se encuentre muy justificado.

No son únicamente los colegios o escuelas los que tienen que preocuparse por ataques de ciberseguridad para filtrar datos educativos, sino también los estudiantes y docentes en sus propios dispositivos, pues la gran mayoría ha estado trabajando en forma remota el último año. Se estima que en Estados Unidos aproximadamente 3 % de los docentes aceptaba sin querer estafas de *phishing*²² al trabajar desde la institución educativa; desde la casa este número ha subido a 15-20 %, lo que le ha dado acceso a muchos cibercriminales a la red escolar ([Krueger, 2021](#)).

Por esta razón se vuelve clave fortalecer la concientización, el conocimiento y el acceso a las herramientas que pueden ayudar a niños y niñas para la protección, privacidad y seguridad de sus datos cuando utilicen plataformas educativas digitales desde cualquier lugar. Además, debe considerarse que esto solo es el inicio del uso de sus datos para fines educativos. Con la acelerada adopción de sistemas de Inteligencia Artificial (IA) —tecnología que requiere un uso masivo de datos—, los datos disponibles en línea se usarán cada vez más para entrenar modelos con distintos fines, por lo que se vuelve aún más fundamental proteger la privacidad y seguridad de la información de los menores en ámbitos educativos, no exponiéndoles a riesgos innecesarios. En este sentido, las plataformas educativas deben seleccionarse en función de la garantía que puedan aportar en la protección que ofrecen de los datos de niñas y niños.

Si bien podemos enfrentar estos riesgos, aún no hay consenso sobre la definición concreta de qué es usar tecnología de manera completamente ética y responsable. Sin embargo, organizaciones alrededor de todo el mundo cada vez le dan más peso a estos temas para que desde un alto nivel —como funcionarios públicos y Ministerios y Secretarías de Educación— pueda proporcionarse orientación para el desarrollo y despliegue de diversas tecnologías. Una de estas iniciativas, que se enfocada específicamente en Inteligencia Artificial, es fAIr LAC, que 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.

Este tipo de iniciativas son excelentes guías para que funcionarios e instituciones puedan consultar pautas, esquemas y guías de implementación tecnológica responsable.

21 Para más información sobre los beneficios y riesgos de la recolección, uso y tratamiento de datos biométricos en instituciones educativas, véanse los siguientes reportes de UNICEF: 1) *Faces, Fingerprints and Feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programmes* (2019), disponible en https://data.unicef.org/wp-content/uploads/2019/10/Biometrics_guidance_document_faces_fingersprint_feet-July-2019.pdf y *Biometrics guidance document faces fingersprint feet-July-2019.pdf*, y 2) *Biometrics and Children: A literature review of current technologies – prepared by UNICEF and the World Bank* (se publicará en 2021).

22 Puede verse una definición de phishing en el anexo 2.

3. Riesgos y retos sistémicos específicos de Latinoamérica para la incorporación de tecnología

A medida que los casos del Covid-19 aumentaron en Latinoamérica, 20 países y 7 dependencias de la región decidieron cerrar progresivamente sus instituciones educativas en todos los niveles. Como resultado, se estima que más de 160 millones de menores de edad se vieron afectados en los niveles preescolar, media y secundaria en toda la región ([Cepal](#), 2020), unos más que otros, según el país.

Una de las lecciones aprendidas de esta pandemia son las ventajas y oportunidades educativas que traen las tecnologías en la educación, que indican una probable alza constante en su adopción en el futuro. Como lo menciona el BID, “el uso de tecnología será una herramienta para la continuidad pedagógica” ([Álvarez, et al.](#), 2020), lo que significa que cada vez más alumnos se conectarán para tomar clases en línea, creando una huella digital exponencial de datos de menores de edad. Por supuesto, para que esto suceda, deben atenderse varios retos en la región: por un lado, retos estructurales que limitan la conectividad de estos estudiantes y, por otro, retos de conocimiento que si no se superan no permitirán que los alumnos sepan aprovechar dicha conectividad para su educación.

La educación digital requiere alfabetización digital. Esta se refiere al nivel de capacidad de una persona para llevar a cabo distintas tareas en el ámbito digital o, en otras palabras, a qué tanto una persona sabe utilizar un aparato digital, comprende cómo su uso puede incrementar la productividad y eficiencia de alguna tarea, identifica los riesgos que puede conllevar y sabe mitigarlos. Antes que nada, se trata de un tema importante para todos los integrantes de una institución educativa: los esfuerzos de digitalización de las operaciones de una escuela serían en vano si no se tuviera el conocimiento suficiente para utilizar adecuadamente tecnologías y herramientas digitales.

La realidad en Latinoamérica es que muy pocos individuos tuvieron la fortuna de conocer los beneficios de la educación digital que se dio como respuesta a los retos educativos que implicó el confinamiento. Incluso los niños y niñas que pudieron quedarse en el sistema educativo se enfrentaron a nuevos retos: tan solo 33 % de los estudiantes de secundaria cursan en instituciones educativas que tienen acceso a internet con suficiente velocidad o ancho de banda. En hogares más vulnerables, este número baja a 22 %, mientras que el promedio reportado en los países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) es más del doble: 68 % ([Álvarez, et al.](#), 2020). El anexo 3 presenta más información acerca del estado de la conectividad general en Latinoamérica, en la que se estima que el acceso a banda ancha de Internet solo llega a 50 % de la región ([Jaramillo](#), 2020).

Si bien la pandemia aportó muchos aprendizajes en el ámbito educativo regional, solo se está viendo la punta del iceberg. Los retos de privacidad de los datos digitales de niños y niñas en ámbitos escolares por ahora no afectan a más de un porcentaje mínimo de la población, pero ese número irá creciendo cada vez más, por lo que la región está en un momento óptimo para empezar a enfrentar los diferentes desafíos que presenta la digitalización de las clases y de la educación en forma más general.

Por otro lado, una alta falta de alfabetización digital agrava los riesgos de privacidad y seguridad de los menores de edad en sistemas SIGED, en el sentido de que los integrantes de una institución educativa solo pueden proteger la privacidad digital de sus estudiantes en la medida en que estén al tanto de los retos a los que se enfrentan.

De hecho, la última Encuesta internacional sobre enseñanza y aprendizaje (TALIS, por su sigla en inglés) de la OCDE en 2019 revela que en la mayoría de los países de Latinoamérica participantes, los docentes consideran que tienen una alta necesidad de formación en herramientas de Tecnologías de la Información y Comunicación (TIC) para la enseñanza ([CEPAL-UNESCO](#), 2020); esta solicitud ocupa el segundo lugar entre las formaciones más demandadas. La Encuesta de Aprendizaje Seguro en Línea LATAM reveló que 72,31 %²³ de los docentes en Latinoamérica no reciben, o es insuficiente, la capacitación necesaria sobre temas de privacidad de datos y uso responsable de plataformas y herramientas digitales.

Recuadro 7. Perspectiva desde los conversatorios y las entrevistas²⁴

Algunos aspectos destacables del ejercicio que se realizó para este reporte fue conversar con docentes²⁵, quienes reconocieron la necesidad de tener mucha más capacitación y conscientización sobre los riesgos que existen en la comunidad educativa latinoamericana en todos los niveles. Además, una pregunta que se realizó en las 15 entrevistas con personas expertas descritas en el apartado de la metodología, en materia de educación a nivel regional e internacional, demostró la falta de priorización del cuidado de la privacidad y seguridad de los estudiantes menores de edad en plataformas digitales. Al preguntarles por qué podría ser, la gran mayoría contestó que tenía que ver con la importancia de otros retos sistémicos que se presentan en el sistema educativo latinoamericano.

En cuanto a la educación de niñas y niños en este tema, existe una gran falta de enseñanza en el tema en las escuelas de Latinoamérica en todos los niveles ([Berríos, et al.](#), 2013). Tampoco los menores de edad pueden contar con el apoyo de sus padres para formarse en habilidades digitales, pues muchas veces los padres no gozan de este tipo de conocimiento ([Subedi](#), 2020). En forma general, esta laguna se debe a la falta de infraestructura y a la insuficiencia de apoyo a la enseñanza de conocimientos digitales en el idioma local y relevantes para el contexto ([GSMA](#), 2016). Esto afecta en particular a las comunidades marginadas y vulnerables, como suelen ser los pueblos indígenas.

23 Cifra tomada de los resultados de la Encuesta de Escuelas en Línea Seguras LATAM sobre la perspectiva de docentes y directores de instituciones educativas acerca de la protección de datos de sus estudiantes.

24 Para conocer más sobre la metodología del conversatorio y las entrevistas, ir a la sección de metodología al inicio del documento.

25 Para más información sobre los conversatorios ver la sección de Metodología de este reporte.

4. Panorama regulatorio y normativa de privacidad de datos en Latinoamérica

La temática de responsabilidad y protección de datos en entornos escolares es aún incipiente, no solo en la región latinoamericana, sino a nivel internacional. De acuerdo con UNICEF, no existe aún una regulación que sea óptima y responda a todas las necesidades de protección y seguridad: “una serie de investigadores y responsables políticos han ofrecido sugerencias relevantes sobre cómo abordar los riesgos para la protección a la privacidad y la equidad que plantean los servicios de tecnología educativa, aunque ninguno abarca todas las preocupaciones relevantes ni ofrece soluciones suficientemente detalladas” ([Barrett](#), 2020).

Las directrices que ofrecen consejos, guías y principios para ayudar a niñas y niños a utilizar los servicios en línea en forma más segura son valiosas y un primer paso en la implementación de protección en escuelas²⁶, **pero los problemas estructurales de gobernanza de datos requieren soluciones específicas para la educación desde sus Ministerios y Secretarías, no soluciones únicamente para los individuos.**

El siguiente análisis de la regulación y normas existentes en Latinoamérica en materia de protección a la privacidad de datos busca ofrecer un panorama del estado del arte la región en el tema.

4.1 Bases para una gobernanza de datos para Ministerios, Secretarías e Instituciones de educación

La gobernanza de datos (GD) es el proceso de gestión de la disponibilidad, la usabilidad, la integridad y la seguridad de los datos en los sistemas de una institución pública, que opera conforme a roles, estándares, normas y/o políticas internas sobre el tratamiento de datos. Una adecuada gobernanza de datos garantiza la eficacia y eficiencia del uso de la información para alcanzar sus objetivos y optimizar sus operaciones.

Un programa de gobernanza de datos bien diseñado suele incluir un equipo de gobierno, un comité directivo que actúa como órgano de gobierno y un grupo de administradores de datos. Estos trabajan juntos para crear las normas y políticas de gobierno de los datos, así como los procedimientos de aplicación y cumplimiento que llevan a cabo principalmente los administradores de datos. Además de los equipos de Tecnologías de la información (TI) de gestión de datos, participan ejecutivos y otros representantes de las operaciones empresariales de una organización.

²⁶ Por ejemplo, la Guía rápida del proyecto Aprendizaje Seguro en Línea, *Guía para instituciones educativas de Latinoamérica para proteger los datos digitales de los niños y las niñas en ámbitos escolares*, del BID y C Minds, 2021.

“Si bien la gobernanza de datos es un componente central de una estrategia general de gestión de datos, las organizaciones deben centrarse en los resultados empresariales (institucionales) deseados de un programa de gobernanza en lugar de los datos en sí”, escribió el analista de Gartner Andrew White en una publicación de su blog de diciembre de 2019. Esta guía sobre la gobernanza de datos explica con más detalle qué es, cómo funciona, los beneficios institucionales que proporciona y los desafíos de gobernar los datos. También incluye una visión general del software de gobierno de datos y las herramientas relacionadas.

¿Por qué es importante la gobernanza de datos en las instituciones educativas?

La gobernanza de datos favorece el uso de los datos de manera responsable para enfrentar los retos que se presentan en el sector educativo. Las instituciones que adopten una gobernanza de datos podrán aprovechar los beneficios de una mejor utilización de los datos en la toma de decisiones.

Los servicios educativos podrán mejorarse aprovechando el tratamiento de los datos sin mermar la protección a la privacidad de sus titulares, por ejemplo, el diseño personalizado de servicios educativos o la elaboración de políticas basadas en proyecciones más sofisticadas y certeras sobre las necesidades de la comunidad estudiantil.

Por otro lado, cuando las instituciones educativas desarrollan políticas, procedimientos y responsabilidades que proporcionan claridad en torno a los datos de los estudiantes y administrativos en cada etapa de su ciclo de vida, prepara el camino para que la información proteja los derechos de privacidad, confidencialidad y seguridad del estudiante o del personal. La siguiente sección explora las bases de regulación que hay en Latinoamérica para sustentar distintos marcos normativos que podrían servir para la gobernanza en instituciones educativas.

4.2 Regulaciones y normas de privacidad en Latinoamérica

Con el objeto de dar a conocer el estado del arte de la privacidad en la región en forma general y resumida, a continuación se presenta un listado e información clave de las últimas actualizaciones de las regulaciones y normas de privacidad en siete países de los más avanzados de Latinoamérica en temas de regulación de privacidad de datos.

Antes de presentar dicha información, y cuando sea posible, aparecen datos sobre el nivel de conocimiento de las personas encuestadas acerca de leyes que protegen la privacidad de los datos en cada uno de los países.²⁷



4.2.1 Argentina

Argentina fue el país pionero en promulgar una de las primeras leyes de protección de datos de la región latinoamericana. Lo hizo en el año 2000. Sin embargo, no se ha actualizado en su mayor parte desde la fecha de su publicación original. La Ley de Protección de los Datos Personales (en adelante LPDP) de Argentina, N° 25.326, que incluye el Decreto Reglamentario N° 1558/2001 y normas complementarias, es una ley federal que aplica a la protección de los datos personales en ese país.

²⁷ Únicamente se incluyeron cifras de los países cuyos números en la Encuesta de *Escuelas en Línea Seguras* LATAM fueran superiores a 240 respuestas.

En 2018, se propuso un proyecto de ley para reemplazar la ley N° 25.326 con una LPDP para alinearse con el Reglamento General de Protección de Datos (RGPD), pero solo hasta 2020 se incluyeron cláusulas adicionales que no se encuentran en el RGPD. En caso de ser aprobada, Argentina tendrá una de las leyes más avanzadas del mundo en cuanto a protección de datos.

Algunas acciones relevantes fueron:

- Cambiar la definición de “disociación de datos” al agregar que “no será considerada persona determinable cuando el procedimiento que deba aplicarse para lograr su identificación requiera la aplicación de medidas o plazos desproporcionados o inviables” (en línea con la Resolución 4/2019 de la Agencia).
- Agregar que el “interés legítimo²⁸” ya no puede ser usado por el Estado como base legal para recopilación de datos.
- Agregar la definición de país adecuado: “un país u organismo internacional o supranacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente”.
- Agregar que en los supuestos de decisiones automatizadas en el marco de la celebración de un contrato o con el consentimiento expreso del titular del dato, el responsable debe adoptar alguna intervención humana para que exprese sus puntos de vista y pueda impugnar la decisión automatizada.
- Incorporar conceptos como “datos genéticos²⁹”, “datos biométricos³⁰” y “computación en la nube³¹”.
- Ampliar el ámbito de aplicación limitado que se refiere únicamente a las personas físicas, excluyendo a las personas jurídicas.
- Obligar a los organismos gubernamentales a nombrar un responsable de la protección de datos si se tratan datos sensibles y de gran volumen. Abordar los derechos adicionales de los interesados. El proyecto de ley reconoce expresamente el derecho a oponerse o restringir el tratamiento y el derecho a la portabilidad de los datos.

28 El interés legítimo es una situación jurídica activa que permite la actuación de un tercero y otorga al interesado la facultad de exigir el respeto del ordenamiento jurídico y, en su caso, de exigir una reparación por los perjuicios antijurídicos que se deriven de esa actuación.

29 Según la [UNESCO](#) (2003) “datos genéticos es la información sobre las características hereditarias de las personas, obtenida por análisis de ácidos nucleicos u otros análisis científicos”.

30 El [Reglamento General de Protección de Datos](#) (RGPD) (2016) los define como: “datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos”.

31 La computación en la nube es el conjunto de todos los recursos computacionales ofrecidos de manera remota y en tiempo real, sin necesidad de mantener un data center local. Están compuestos por una serie de servidores para dividirse los recursos ([IBM](#), s.f.).



4.2.2 Brasil

En agosto de 2018, Brasil aprobó su primera regulación en materia de datos personales, que entró en vigor en septiembre de 2020. Se redactó tomando como modelo el RGPD europeo. Hasta hace muy poco, Brasil carecía de una ley específica para regular los aspectos de protección e identificación de datos en el entorno digital; incluso, carecía de una definición de “datos personales”.

Ello no significa que Brasil hubiera dejado a su población sin regulaciones para protección de datos, sino que estas se encontraban en códigos de otras materias como, por ejemplo, el Código de Protección del Consumidor, que concedía algunos derechos de privacidad para acceder y corregir los datos de los consumidores, así como el Código Penal, que imponía algunas sanciones al mal uso de datos, y el Marco Civil de Internet, aprobado en 2014, uno de cuyos principios es la privacidad.

Algunos datos relevantes de la Ley General de Protección de Datos son:

- Tiene 10 bases jurídicas para el tratamiento lícito de datos.
- Crea figuras de autoridad de datos: responsabiliza a las compañías y organizaciones de nombrar un Oficial de Protección de Datos (OPD) y confiere a la Autoridad Nacional de Protección de Datos (ANPD, *Autoridade Nacional de Proteção de Dados*) apoyar a otras secretarías y organismos públicos.
- Aplica en ambos sectores: privado y público.
- Marca límites territoriales, es decir, si los datos se procesan o manejan en Brasil, están sujetos al tratamiento responsable.
- Crea la posible imposición de multas de hasta 2 % de los ingresos brutos de una empresa en Brasil en el último ejercicio fiscal por incumplimiento.
- Incluye un artículo específico sobre la protección de datos de niños y adolescentes, considerada como una prioridad absoluta, de acuerdo con la Constitución federal.



4.2.3 Chile

Al día de hoy, la actualización de la ley de protección de datos personales en Chile (promulgada como Ley 19.628 en 1999) se encuentra en la fase final de revisión en la Comisión Constitucional del Senado. Su objetivo era establecer disposiciones generales sobre los datos personales tratados por terceros privados. La actualización busca establecer cuáles son los mecanismos e instrumentos para implementar la manera como los titulares de los datos deben ser informados sobre las finalidades del tratamiento de su información personal y que se debe recabar su consentimiento.

Este proyecto de ley:

- Regula la protección y el tratamiento de los datos personales.

- Crea un Consejo de protección de datos para hacer cumplir la ley e impone multas de hasta 700.000 dólares.
- Introduce los datos biométricos en la definición de datos sensibles.

Es de gran importancia mencionar que Chile también ha acordado modificar su Constitución para incluir el derecho de protección de datos personales.



4.2.4 Colombia

De las 322 personas encuestadas en Colombia, solo 66 % conoce alguna ley que proteja la privacidad de niños y niñas.

Si bien Colombia cuenta con un marco robusto de protección de datos enmarcado en la Constitución, concretado en 24 leyes, 14 decretos en temas de internet, además de otras disposiciones de ciberseguridad, privacidad y de IT (entre ellas el Habeas Data), también es cierto que el gobierno tiene en la mira actualizar e incorporar nuevas cláusulas a sus actuales leyes de protección de datos, las leyes N° 1581 y N° 1266, con disposiciones pertinentes que aborden las innovaciones tecnológicas contemporáneas.

Uno de los temas más importantes en Colombia es el proyecto de ley que pretende dotar a la Ley de privacidad de datos, N° 1581, del alcance internacional del RGPD, de modo que incluya aspectos como:

- Adición de nuevas definiciones de datos sensibles, datos públicos y aviso de privacidad.
- Especificación de ciertos requisitos para las políticas de privacidad.

En 2017, Colombia creó una lista de “adecuación” ([Valbuena Abogados](#), 2017) para las transferencias transfronterizas, que contiene una lista de países que cumplen los estándares de nivel de protección de datos adecuados según los criterios colombianos.



4.2.5 México

De las 319 personas encuestadas en México, solo 52 % conoce alguna ley que proteja la privacidad de niñas y niños.

México tiene dos leyes de protección de datos personales: la de 2010, que afecta a “privados”, y la del 2017, que afecta a “sujetos obligados” (entidades públicas federales, estatales y municipales). En abril de 2010 se promulgó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que es la base de un sistema integral de privacidad que regula el tratamiento de los datos personales, y que incluye su recolección, uso, transferencia y almacenamiento. En virtud de estas dos leyes, se concede a los interesados derechos como el acceso, la rectificación, la cancelación o la oposición al tratamiento de datos.

México tiene una institución que es la autoridad en uso de datos: el Instituto Nacional

de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Entre enero de 2012 y enero de 2017 el INAI ha impuesto sanciones a empresas que operan en México en 147 casos, por un importe total de aproximadamente 16,7 millones de dólares.

Al día de publicación de este reporte, la última actualización de datos fue en noviembre de 2020. Integra en el acuerdo vigente la aprobación de la adición de un Título Décimo a los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

En general, el Código de Protección de Datos contiene:

- Procedimientos de Protección de Derechos ARCO³².
- Reclamaciones presentadas por los titulares de los datos.
- Procedimientos de verificación. Además, el INAI es posiblemente la autoridad de protección de datos más activa de Latinoamérica.
- Adhesión reciente de México al Convenio Europeo para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal ("Convenio 108").
- Promulgación de dos guías: la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales y la Guía para el Tratamiento de Datos Biométricos.



4.2.6 Perú

De las 245 personas encuestadas en Perú, 50 % ubica alguna ley que proteja la privacidad de niños y niñas.

En 2011, Perú promulgó la Ley N° 29.733, cuyas disposiciones buscan una amplia protección y otorgan derechos adecuados a los interesados en caso de que las empresas que procesan datos personales no cumplan sus obligaciones.

La ley de protección de datos en Perú se actualizó recientemente para ampliar las directrices legales para el tratamiento de datos y reforzar su régimen de protección de datos e incorporó algunas disposiciones relevantes, relacionadas con la transferencia de datos:

- Señala que el responsable del tratamiento está obligado a notificar cualquier transferencia de datos resultante de las fusiones y adquisiciones de una empresa y a inscribir las transferencias internacionales de datos en un registro nacional peruano.
- Incluyen nuevas exenciones a la obtención del consentimiento para el tratamiento de datos, principalmente para prevenir el blanqueo de capitales y la financiación del terrorismo.

³² En los países latinoamericanos, los derechos ARCO se refieren a aquellos derechos que tiene un titular de datos personales para solicitar el acceso, rectificación, cancelación u oposición sobre el tratamiento de sus datos ante el Sujeto Obligado que esté en posesión de los mismos.



4.2.7 Uruguay

En agosto de 2008, Uruguay promulgó la ley de Protección de Datos (Ley 18.331). Además, cuenta con una institución que es autoridad en materia de digitalización, la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC), así como una Unidad Reguladora y de Control de Datos Personales (URCDP).

En enero de 2019 entró en vigencia la nueva Ley de Rendición de Cuentas, que incorpora importantes modificaciones a la legislación nacional sobre protección de datos personales, con el fin ofrecer mayores garantías a los uruguayos. Es la autoridad de control, un órgano desconcentrado con autonomía técnica, cuya competencia es custodiar el cumplimiento de la legislación de protección de datos personales y el respeto de sus principios. La Unidad tiene como cometidos asesorar al poder ejecutivo y recomendar políticas en el tratamiento, seguridad y manipulación de datos personales. Este organismo es importante en la protección de datos en ámbitos escolares porque trabaja de la mano del Ministerio de Educación y el Plan Ceibal para asegurar el manejo responsable de sus datos.

Además, con sus normas, AGESIC:

- Establece que el consentimiento informado debe ser libre (podrá brindarlo o no), previo (recabado antes de solicitar los datos), expreso (no tácito o implícito), documentado (verificable) e informado (conocer la finalidad para la que se recolectan los datos y dónde ejercer sus derechos).
- Contempla el principio de veracidad. Los datos registrados deberán ser veraces, adecuados, ecuanímenes (imparciales) y no excesivos en relación con la finalidad para la que se han obtenido. Será excesivo, por ejemplo, si se requiere preferencia política para afiliarse a un club deportivo.
- Tipifica los datos sensibles y prohíbe su compartición obligatoria.
- Identifica datos que por sus características deben ser especialmente protegidos: datos sensibles, datos de salud, datos relativos a las telecomunicaciones, datos relativos a bases de datos con fines publicitarios y datos relativos a la actividad comercial o crediticia.



Iniciativa de Ley de Privacidad de Datos de El Salvador

En el momento de redacción de este escrito, El Salvador presentó en abril de 2021 en la Asamblea Legislativa de la República, el Decreto N° 875, también conocido como la Ley de Protección de Datos Personales y Hábeas Data. La normativa se complementará con otras dos leyes cuyo enfoque es la protección de derechos de autor —que es la Ley de Fomento de la Economía Creativa, conocida como “Ley Naranja”—, y la Ley de Creación de la Autoridad Nacional Digital para la gobernanza de datos.

A continuación aparecen varios aspectos destacables de la propuesta de legislación:

- Se reconocen e incluyen definiciones de los términos de autodeterminación informativa, base de datos o repositorio, bloqueo de datos, consentimiento, dato personal, dato sensible, persona designada para el tratamiento de datos, disociación o anonimización, persona designada para del tratamiento, fuentes de acceso público, seudonimización y transferencia de datos personales, entre otros.
- Se reconocen nueve principios para la protección de datos: principio de legalidad, principio de calidad, principio de lealtad, principio de consentimiento y finalidad, principio de minimización de datos, principio de calidad, principio de transparencia, principio de seguridad de datos y principio de privacidad.
- Además de los Derechos ARCO, se incluye el derecho a la portabilidad, así como pautas para la transferencia internacional de datos personales.
- Se determinan las características que deberían tener las bases de datos de instituciones públicas y de titularidad privada y pública.

Parte del aspecto pionero de esta propuesta es que se crearía una nueva institución gubernamental para vigilar estas leyes: la Autoridad Nacional Digital, una institución de derecho público, con personalidad jurídica, patrimonio propio y con autonomía administrativa y presupuestaria. Tendrá competencia en la administración pública y en las oficinas privadas.

Como lo muestra esta sección, Latinoamérica cuenta con bases para crear marcos de gobernanza y normativas de privacidad, pero aún existe una gran oportunidad para enfocar las regulaciones en los ámbitos escolares y en los menores de edad.

4.3 Mejores prácticas para fortalecer la privacidad de niños y niñas en entornos educativos digitales

La evolución normativa es un proceso natural en todo Estado de derecho. En la medida en que la sociedad se va transformando y los individuos van adoptando nuevas formas de relacionarse, las disposiciones legales se adecuan para contemplar nuevos escenarios o entornos que anteriormente no se consideraban. Tratándose de regulaciones tan sensibles como la privacidad de los menores de edad en el entorno digital, la mejora regulatoria debería enfocarse en la mitigación extrema de riesgos para los titulares de los datos, así como en las acciones que permitan minimizar las brechas preexistentes en la región en relación con la protección de datos personales. También deja la puerta abierta a actores de otros países con legislaciones más avanzadas para que tomen ventaja de las lagunas legales en la región.

A continuación aparece un ejemplo de caso de regulación en Estados Unidos, que promueve la protección de datos en ámbitos escolares. Muestra cómo la privacidad de datos de menores puede regularse desde distintos frentes para atender diversas necesidades e

involucrar una variedad de agentes relevantes. Las investigadoras consideran que esta es la regulación más robusta en temas de privacidad de datos de niñas y niños, pues cubre el trato de datos desde los sectores privado y público y establece de qué manera los funcionarios públicos y docentes deben interactuar y cuidar los datos.

Recuadro 8. Breve resumen de CIPA, COPPA y FERPA

- 1. Ley de Protección de la Infancia en Internet** (CIPA, por sus siglas en inglés). Esta ley regula el filtrado del acceso a Internet, el uso aceptable y la educación cívica digital. Obliga a la Comisión Federal de Comunicaciones (FCC) y a la Supervisión del distrito educativo a responsabilizarse por:
 - a. Los Servicios de Tecnología que gestionan las medidas de protección de la tecnología;
 - b. El personal del distrito, incluidos los docentes y el personal de apoyo, la supervisión del uso estudiantil de los recursos tecnológicos del distrito y la educación de los estudiantes sobre el comportamiento adecuado en línea.
- 2. Ley de Protección y Privacidad de los Niños en Internet** (COPPA, por sus siglas en inglés). Esta ley regula la recopilación, el uso y la divulgación de la información personal de niñas y niños menores de 13 años. Esta ley debe cumplirla cualquier persona, incluso los docentes, que seleccione y evalúe recursos en línea, sitios web y aplicaciones que vayan a utilizar estudiantes menores de 13 años. El mandato incluye a directores y actores gubernamentales.
- 3. Ley de Derechos Educativos y Privacidad de la Familia** (FERPA, por sus siglas en inglés). La ley protege la privacidad de los registros educativos estudiantiles y se aplica a todos los que tienen acceso a los expedientes académicos. FERPA exige a las instituciones y agencias educativas que obtengan un permiso por escrito de los padres o del estudiante elegible para poder divulgar cualquier información de su expediente educativo. Las instituciones y agencias educativas también deben notificar anualmente a los padres y estudiantes mayores de 18 años sus derechos en virtud de la FERPA y proporcionarles tiempo suficiente para solicitar que no se compartan los registros estudiantiles. También proporciona a los padres o estudiantes mayores de 18 años derechos a:
 - a. Inspeccionar o revisar los registros educativos del estudiante, que mantiene la escuela, en un plazo de 45 días a partir de la solicitud.
 - b. Solicitar la modificación de los registros educativos que se consideren inexactos.
 - c. Consentir la divulgación de la información de identificación personal de los registros educativos, salvo lo especificado por la ley.

Como muestra este ejemplo, es deseable tener marcos jurídicos que se ajusten a las distintas necesidades de protección de datos, dependiendo de los actores involucrados. Ya sea con la creación de leyes específicas o la adaptación de la existente que contemple distintas dimensiones, se ha observado que las normas de privacidad pueden complementarse con enfoques específicos para la protección a los derechos de los menores.

Si bien en Latinoamérica no se cuenta con leyes similares, cada vez más se fortalecen las regulaciones en el ámbito de la privacidad, como se refleja en la sección anterior de resumen de regulaciones y normas. Sin embargo, es necesario detenerse a ajustar estas leyes, dependiendo de las necesidades de cada país o región.

Existen otros ejemplos de regulaciones de protección y privacidad de datos, como el GDPR. Sin embargo, su enfoque no especifica ámbitos educativos, sino que se refiere al uso de redes sociales en general.

Recuadro 9. Artículo 8 del GDPR

En relación con la oferta directa a niños y niñas de servicios de la sociedad de la información, el tratamiento de los datos personales de un joven se considerará lícito cuando tenga como mínimo 16 años. Si la persona es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

A continuación, a partir del análisis presentado y las oportunidades y retos identificados para mejorar la privacidad de niñas y niños en ambientes escolares, se ofrece una serie de recomendaciones a modo de guía para el abordaje del tema desde los gobiernos, principalmente de los Ministerios y Secretarías de Educación.

5. Recomendaciones

A través de las líneas de acción propuestas se tiene como objetivo que la implementación de la tecnología en entornos educativos beneficie a todos los estudiantes, sin poner en riesgo su seguridad y privacidad. Estas recomendaciones se presentan para los gobiernos, con un enfoque especial en los Ministerios y las Secretarías de Educación de Latinoamérica, así como para las autoridades nacionales de protección de datos, legisladores, organizaciones de la sociedad civil, instituciones especializadas en educación de los sectores público y privado, asociaciones escolares de padres y madres de familia y otros actores que juegan algún rol dentro de la adopción de tecnologías basadas en datos para niños y niñas en el ámbito educativo, de modo que puedan explorar su adopción, existan mecanismos para que sean vigentes ante cambios de gobierno o que puedan darle seguimiento aunque haya cambio de gobierno.

Es importante reconocer la pluralidad de voces que forman parte del ecosistema educativo. Por lo tanto, las recomendaciones toman como punto de partida la participación multisectorial y los esfuerzos desde distintas perspectivas: docentes, padres de familia, estudiantes, funcionarios de gobierno y autoridades de datos, entre otros. Cada recomendación incluye el actor sugerido para llevar a cabo la actividad.

Asimismo, estas recomendaciones no se presentan en ningún orden en particular, porque todas incluyen acciones cruciales para fortalecer la privacidad de niñas y niños en ámbitos escolares digitales y, por lo tanto, se recomienda llevarlas a cabo en forma paralela, en la medida de lo posible.

Las recomendaciones en un vistazo





5.1 Promover una estructura organizacional y gobernanza de datos a través del desarrollo de marcos normativos y regulatorios

1. Reformar la legislación para actualizarla y adecuarla a las necesidades de protección, seguridad y privacidad de datos de la niñez, comenzando por ámbitos educativos (Autoridad de Educación y/o de Datos o Datos personales).

Si bien la región tiene avances significativos en materia de legislación de privacidad, es apremiante que se creen marcos normativos y, eventualmente, regulatorios que contemplen y cuya prioridad sea la participación de las instituciones educativas, teniendo en el centro al menor estudiante, con el propósito de poner lineamientos y límites para el uso de plataformas digitales, tanto para privados como para servicios públicos e instituciones educativas.

A la par de integrar tecnología y plataformas educativas a las reformas educativas de las siguientes décadas, los gobiernos podrían considerar la generación de marcos de uso y actualizar la normativa de protección de datos para que estos reconozcan el derecho a la privacidad de los estudiantes. En ellos deberían incluirse las normativas que rijan el uso de la tecnología de vigilancia y protección especial de datos biométricos.

Los lineamientos tendrían por objeto orientar a directores y docentes en el uso de tecnologías en ámbitos escolares. Las leyes no son el único medio a través del cual puede lograrse esta política pública; también a través de códigos, normas, estándares y el establecimiento de buenas prácticas puede darse una gobernanza más amplia y completa a la protección, privacidad y seguridad de los datos de los estudiantes.

2. Crear reglamentos y normas para la recolección y uso de datos (Autoridad de Educación y/o de Datos).

Cada país podría generar un marco regulatorio que redunde en la protección de datos digitales de la niñez, lo cual incluye un análisis exhaustivo de las reales y posibles normativas de privacidad y tecnologías emergentes. Como región, Latinoamérica podría tener convenciones para intercambiar conocimiento y buenas prácticas sobre este tema, pues tiene desafíos que son únicos y específicos en los derechos de protección y seguridad de datos de estudiantes y menores.

Los países que cuentan con bases legales para la privacidad podrían actualizar la legislación. A su vez, la aproximación a la protección, privacidad y seguridad de datos no solo debería ser desde las leyes, sino que pueden acordarse lineamientos, estándares y principios para el uso de datos en ámbitos educativos para complementar la futura regulación.

3. Crear grupos de trabajo interinstitucionales para tomar los primeros pasos hacia la creación de una Autoridad de Datos, si es que el país no la tiene (Gobierno).

Es fundamental que para darle la correcta importancia y protección a los datos personales exista una autoridad competente encargada de vigilar y salvaguardar dicha información (sobre todo cuando esta es sensible) para que no se utilice indebidamente, se respeten los derechos y se vele el debido cumplimiento de la legislación aplicable, así como su desarrollo. A su vez, este grupo debe enfocarse en detectar las necesidades locales, estudiar las buenas prácticas internacionales y tener en cuenta las perspectivas de diversos grupos de interés del sector educativo para integrar una ruta de acción que atienda la problemática. Este grupo podrá coordinar propuestas de actualización o creación de regulaciones necesarias, entre otras estrategias pertinentes que identifique.

Es importante que puedan crearse mecanismos de coordinación, como comités de alto nivel intersecretariales, que congreguen a los responsables y líderes de cada tema para poder avanzar hacia un modelo educativo híbrido (presencial y digital) que no ponga en riesgo a los estudiantes por falta de enfoque en la privacidad y seguridad de sus datos. El Comité buscaría avanzar acciones, políticas y leyes relevantes para proteger la privacidad de los datos digitales de niños y niñas en ámbitos escolares, a medida que vaya creciendo el alcance de las plataformas digitales educativas. Esto es particularmente relevante dada la adopción incremental de nuevas tecnologías basadas en datos para la educación.

Para países que no tengan autoridad de protección de datos se recomienda explorar la creación de un organismo público. El siguiente recuadro presenta un caso en Latinoamérica: el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) de México.

Recuadro 10. Caso de uso: El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)³³.

El INAI es un organismo público autónomo mexicano cuyos objetivos son garantizar el acceso a la información pública y la protección de los datos personales, así como promover la transparencia de la administración pública y su rendición de cuentas. El Instituto es responsable de asegurar el cumplimiento del derecho a la protección de datos personales y tiene la facultad de difundir la información sobre este derecho, así como promover el ejercicio de los derechos de acceso, rectificación, cancelación y oposición (ARCO) que tiene toda persona con respecto a su información personal.

El INAI cuenta con una serie de guías para proteger los datos personales de menores, por ejemplo, ha emitido recomendaciones a padres, madres y tutores para que protejan los datos durante las inscripciones escolares en línea (Zepeda, 2021). Asimismo, a través de actividades interactivas, como juegos, concursos e historietas, entre otros (INAI, s.f.), busca que niños, niñas y adolescentes tengan información sobre qué son sus datos personales y cómo protegerlos.

33 Para más información acerca de esta institución, visite la página oficial: <https://home.inai.org.mx/>

4. Explorar los beneficios y riesgos de la IA y otras nuevas tecnologías basadas en el uso masivo de datos (Autoridad de Educación y/o de Datos, Academia, Sociedad Civil).

Tal como se mencionó, la IA ofrece beneficios considerables para el sector educativo, pero también riesgos para las partes interesadas. Se recomienda que se lleven a cabo investigaciones y pilotos para entender cómo aprovechar los beneficios de esta tecnología, así como otras tecnologías basadas en datos, sin caer en sus riesgos.

A la vez, se vuelve interesante explorar cómo integrar a los planes nacionales de IA elementos que atiendan a los menores de edad, en los ámbitos personal y educativo.



5.2 Fomentar el desarrollo de capacidades

1. Promover la educación y campañas de concientización en el tema a todos los niveles (Autoridad de Educación y/o de Datos o Sociedad Civil).

Los datos recopilados en la Encuesta de Aprendizaje Seguro en Línea LATAM muestran que menos de 50 % de los docentes de Colombia, México y Perú³⁴ saben que existe una ley de protección de datos de los menores de edad. Esto demuestra que aún queda trabajo por realizar en el aumento de conciencia en torno a un elemento que se ha vuelto central en la educación y en la protección de niños y niñas en ámbitos educativos: la ciberseguridad y la importancia de fortalecer la educación y campañas de concientización en el desarrollo de capacidades digitales, como ya se viene implementando en otros países

2. Facilitar cursos para una navegación segura en línea, diferenciados por perfiles (Autoridad de Educación y/o de Datos o Sociedad Civil).

Para cada actor distinto (estudiantes, docentes, padres de familia y funcionarios públicos) se recomienda ofrecer o facilitar el acceso a cursos de ciberseguridad enfocados en los retos enfrentados en el ámbito educativo y, si se desea, también en el ámbito personal, para que reduzcan su exposición a los riesgos del mundo digital. Esto incluye a tomadores de decisión y funcionarios públicos. Debería incorporarse la temática de tecnologías disruptivas y ciberseguridad en las capacitaciones de los reguladores. A su vez, esta meta puede lograrse a través del impulso de campañas de educación sobre la temática, así como de la organización de eventos, conferencias y oferta de clases públicas en la materia. Este último punto puede realizarse en colaboración con asociaciones de la sociedad civil o empresas.

Cada herramienta de desarrollo de competencias y habilidades debe enfocarse en responder a las necesidades de cada agente y a la realidad de su contexto. Uno de los retos más importantes que enfrentan los actores de la región para solucionar este reto es la falta de información sobre el tema, porque no existen métricas para evaluar el alfabetismo digital.

³⁴ Estos son los tres países participantes en la Encuesta de Escuelas en Línea Seguras LATAM que cuentan con regulación de privacidad de datos. Representan más de 880 respuestas.

Recuadro 11. Caso de uso: capacitación desde el gobierno de Brasil.

El gobierno brasileño generó capacitaciones digitales para que docentes, directivos y distritos escolares supieran cómo hacer un manejo responsable de datos escolares de estudiantes y demás personal educativo. Este contenido es gratuito y está disponible en cualquier momento para que toda persona pueda acceder a capacitarse en estos temas:

- <https://dadosestudantis.org.br/>
- <https://internetsegura.br/>
- <https://nic.br/videos/categoria/seguranca/>

3. Desarrollar un directorio de personas expertas en temas relevantes para la protección de datos digitales de menores en ámbitos escolares y materia de privacidad, ética, datos y plataformas digitales educativas (Autoridad de Educación y/o de Datos, Academia y/o Sociedad Civil).

Para que los países de la región puedan crear estrategias de protección de datos en ámbitos escolares es necesario contar con una fácil identificación de los especialistas, personas expertas y organizaciones claves en la región. Esto puede presentarse como un reto por la novedad del nivel de intersección entre el mundo educativo y el mundo digital, por lo que se recomienda identificar los temas relevantes (por ejemplo, privacidad, ética, datos, educación, entre otros) y generar un directorio de personas expertas a nivel regional que puedan apoyar en diferentes instancias.

Dada la diversidad de leyes de protección de datos en los países latinoamericanos se recomienda que estos directorios se realicen a nivel nacional. Además, y como lo dice el *Manifiesto de Gobernanza de datos de menores de UNICEF* ([UNICEF](#), 2021), se debe reconocer la agencia que ejercen los menores sobre sus datos y debería integrarse su participación en los mecanismos de gobernanza de datos.

4. Fortalecer la comunidad de práctica educativa latinoamericana (Autoridad de Educación y/o de Datos y/o Sociedad Civil).

Para fortalecer el ecosistema en la región podría considerarse la generación de una coalición para la colaboración e intercambio de conocimiento y experiencias que tenga por objetivo promover la protección de datos digitales de menores en ámbitos escolares. Se reunirían personas de los países de la región desde todos los sectores: la sociedad civil, la academia y los sectores público y privado en torno a distintas temáticas de interés para compartir perspectivas, casos de estudio y aprendizajes. Se recomienda apoyarse en organizaciones multilaterales e iniciativas existentes³⁵.

35 Por ejemplo, la iniciativa fAIr LAC del Banco Interamericano de Desarrollo.

Recuadro 11. Caso: Coalición de comunidad educativa enfocada en el uso de tecnología (UNESCO, 2020).

La Coalición Mundial por la Educación es una iniciativa impulsada por la UNESCO que reúne a más de 175 países miembros de la ONU, organizaciones de la sociedad civil, academia y sector privado, a través de una plataforma de colaboración e intercambio de conocimiento para la protección del derecho a la educación, durante y después de la situación actual.

Esta plataforma tiene tres pilares principales: la conectividad, los docentes y la igualdad de género. El objetivo es responder y crear soluciones ante los diferentes desafíos que presenta mantener el aprendizaje en el contexto actual.

Gracias a la coalición se han desplegado diferentes esfuerzos conjuntos ([Pion Education](#), s.f.) a través de apoyos, herramientas educativas y tecnológicas para más de 70 países. Entre estos esfuerzos se encuentran, por ejemplo, plataformas para permitir que estudiantes de escuelas públicas puedan tener acceso a la educación, incluso sin tener internet.



5.3 Invertir en infraestructura tecnológica para la aplicación de las normas

1. Invertir en la infraestructura necesaria para que servidores y proveedores públicos y privados puedan cumplir las normas y marcos de protección, privacidad y seguridad de datos.

Se recomienda identificar a las partes interesadas en el ámbito educativo, así como las diferentes temáticas clave que se requieren para crear un grupo de trabajo que abarque los diferentes aspectos clave de la educación. El Grupo de Trabajo³⁶ ofrecería un espacio para que actores del ecosistema educativo no gubernamental tengan la oportunidad de compartir sus preocupaciones y explorar, en forma colaborativa, posibles soluciones.

³⁶ Para conocer más acerca de cómo podría conformarse un grupo de trabajo, véase la recomendación 3 del numeral que titene por título: 5.1. Estructura organizacional y gobernanza de datos a través de marcos normativos y regulatorios.

**Recuadro 12. Caso de uso: Datos de los niños y privacidad en línea. Cre-
cer en la era digital³⁷**

Este proyecto, dirigido por la profesora Sonia Livingstone, trata de abordar las cuestiones y las lagunas de los datos relativos a la concepción de la privacidad en línea por parte de niñas y niños, su capacidad para dar su consentimiento, sus habilidades funcionales (por ejemplo, para entender los términos y condiciones o para gestionar la configuración de la privacidad en línea) y su comprensión crítica más profunda del entorno en línea, incluyendo sus dimensiones interpersonales y, especialmente, las comerciales (que incluyen los modelos de negocio, los usos de los datos y los algoritmos, las formas de reparación, los intereses comerciales, los sistemas de confianza y la gobernanza).

Este proyecto cuenta con el apoyo de varias instituciones del gobierno del Reino Unido, como la Oficina del Comisario de Información, que identifica las oportunidades de inversión tecnológica para el país.

2. Establecer estándares para que en cualquier proceso de contratación pública se respeten los lineamientos y estándares de protección, privacidad y seguridad de datos³⁸.

Las adquisiciones, arrendamientos, servicios y obras públicas del gobierno que lleven a cabo las dependencias gubernamentales deberían contemplar como requisito cumplir los estándares establecidos de seguridad, protección y privacidad de datos, se realicen por licitación, invitación o adjudicación directa.

3. Establecer protocolos de seguridad en ambientes educativos (Autoridad de Educación y/o de Datos).

Si bien se debe reconocer cierta autonomía de los estudiantes menores de edad en la protección de la privacidad de sus datos según su edad, desde el gobierno se recomienda establecer protocolos claros con lineamientos para la protección y privacidad de los datos por parte de todos los agentes de interés en su tratamiento y uso: distritos, personal administrativo de educación, docentes y cualquier actor que tenga acceso o contacto autorizado con la información personal de los estudiantes.

Para poder lograr la protección, privacidad y seguridad de los datos se necesitará invertir para que el Ministerio tenga la tecnología adecuada para llevar a cabo sus funciones de monitoreo, gobernanza y administración electrónica y digital.

37 Título original: Children's data and privacy online: Growing up in a digital age.

38 Para conocer más acerca de las mejores prácticas de contratación pública recomendamos el texto de Políticas para la Adquisición de Bienes y Obras financiadas por el Banco Interamericano de Desarrollo (BID: Marzo 2011). <https://idbdocs.iadb.org/wsdocs/getdocument.aspx?docnum=774396>

Recuadro 13. Guía para instituciones educativas de Latinoamérica para proteger los datos digitales de niñas y niños en ámbitos escolares³⁹

Esta es una guía ejecutiva, desarrollada en el marco del presente proyecto, para instituciones educativas donde pueda agilizarse la consulta de una utilización responsable y ético de los datos de estudiantes en Latinoamérica en el uso de plataformas digitales educativas. Esta guía comparte información accionable; por ejemplo, machotes para la autorización de datos de los alumnos, lista de control de un uso responsable de los datos personales en temas de privacidad y guía de comunicación, entre otros.



5.4 Fomentar políticas complementarias en temas de conectividad, brecha digital e inclusión

1. Fortalecer la conectividad del país e invertir en su calidad para fines educativos (Autoridad de Telecomunicación y de Educación).

Los gobiernos deberían desarrollar un plan para priorizar la infraestructura para el acceso escolar digital. Es decir, seguir invirtiendo en el desarrollo de infraestructura digital orientado específicamente al sector educativo para ofrecer conectividad de calidad a los estudiantes hasta en las zonas más remotas del Estado ([BID](#), 2015). A su vez, pueden explorarse colaboraciones público-privadas para lograrlo, como se ha realizado en varios países con empresas multinacionales de tecnología.

A continuación se presenta un caso de uso:

Recuadro 14. Caso de uso: Plan Gratuito de Telefonía en Perú

A partir de la pandemia del Covid-19 el Ministerio de Educación de Perú, junto a las Direcciones Regionales de Educación y las Unidades de Gestión Educativa Local, y las empresas telefónicas presentes en el país, crearon un plan gratuito de telefonía y datos llamado [Recarga Minedu](#). Gracias a este plan fue posible que más de 400.000 docentes, directivos y personal administrativo educativo pudieran tener datos sin ningún costo. Gracias a las compañías telefónicas los docentes, mediante llamadas, mensajes de texto o aplicaciones de mensajería instantánea pueden seguir el proceso de acompañamiento y estar en comunicación con estudiantes en el marco de la estrategia [Aprendo en casa](#).

2. Analizar a profundidad los impactos de la brecha digital en el entorno educativo, en contexto del Covid-19 (Gobierno, Academia y/o Sociedad Civil).

Si bien ya existen cifras preliminares y especulaciones de las consecuencias de la pandemia en la educación, es recomendable que cada país analice su impacto en la

³⁹ Guía rápida del proyecto: Aprendizaje Seguro en Línea. *Guía para instituciones educativas de Latinoamérica para proteger los datos digitales de los niños y las niñas en ámbitos escolares*, del BID y C Minds, 2021.

educación y en particular en la evolución de la brecha digital. Esto debería hacerse con el objetivo de identificar los siguientes pasos clave que conviene dar en la implementación de infraestructura digital y las métricas que marcarán el progreso de este desarrollo.

3. Desarrollar estrategias de inclusión focalizadas a grupos y comunidades marginadas y vulnerables, como suelen ser los pueblos indígenas (Autoridades de Educación e Instituciones y Organismos de Inclusión).

La inclusión de tecnología en los ámbitos escolares indígenas representa una oportunidad para avanzar el desarrollo social, económico y ambiental en una forma alineada con los valores de los pueblos indígenas de la región ([Cotacachi, et al., 2020](#)). Una estrategia de integración digital no estará completa si no contempla el tema central de la inclusión.

El siguiente recuadro presenta un ejemplo de actividades regulares que puede realizarse para fomentar su inclusión.

Recuadro 15. Caso de uso: Capacitación digital para comunidades indígenas

Desde 2015, la Unión Internacional de Telecomunicaciones (UIT), junto con otras instituciones y organizaciones que apoyan los derechos de los pueblos indígenas, realiza una serie de programas de formación para líderes indígenas. Esta capacitación incluye una fuerte agenda de alfabetización digital y desarrollo de habilidades computacionales. Sus programas ayudan a fortalecer las habilidades de minorías y grupos vulnerables. De esta manera las tecnologías se hacen accesibles y logran ser herramientas democratizantes en la región.

6. Conclusión

A raíz de la pandemia del COVID-19 el uso de plataformas educativas y sistemas SIGED ha ido en aumento, permitiendo a millones de alumnos alrededor del mundo continuar sus estudios. A nivel global, se vio la tendencia de usar tecnologías para darle continuidad a la educación de miles de millones de estudiantes. Sin embargo, desde antes de la pandemia, el uso de tecnología en las aulas ya iba en aumento; podría decirse que la pandemia solo aceleró el proceso de integración de la tecnología en los ámbitos escolares. Además, así como la Inteligencia Artificial ha permeado en diversos servicios, como finanzas y procesos industriales, la educación no es la excepción, pues es uno de los ámbitos donde se presenta la implementación y la conveniencia del cada vez más recurrente uso de esta tecnología ([BID](#), 2020).

Entre muchas otras cosas, la IA ofrece la posibilidad de personalizar el aprendizaje con herramientas complementarias a la educación que se brinda en forma presencial. Para Ministerios y Secretarías de Educación, la tecnología representa una oportunidad para superar brechas educativas; tanto las plataformas educativas como los sistemas SIGED aportan muchísimos beneficios a los estudiantes.

Aunque, en general, el auge del uso de tecnología en los ámbitos educativos ha traído muchos beneficios para estudiantes, docentes, padres y madres de familia, tutores, directivos y demás personal educativo, es preciso considerar que su uso también conlleva riesgos; entre ellos, los riesgos de protección, privacidad y seguridad de datos.

Como se ha mostrado a lo largo de este reporte, la protección, privacidad y seguridad de los datos es un tema clave y decisivo para el futuro de la educación. Es un reto que irá aumentando con la creciente adopción de plataformas educativas digitales y nuevas tecnologías basadas en datos, como la IA. Las alianzas entre Secretarías y Ministerios de Educación con las autoridades de protección de datos, sector público, academia y demás organizaciones marcará las pautas para crear ámbitos escolares y de aprendizaje seguros en línea, que vayan a la par con el aprovechamiento tecnológico dentro de las aulas.

Ante la digitalización de los procesos y actividades escolares, aunada a la cantidad y el valor de los datos que resguardan las instituciones educativas, estas ya han sufrido un incremento exponencial en el número de ciberataques desde el inicio de la pandemia. La protección, privacidad y seguridad de datos presenta riesgos específicos en Latinoamérica, dada la brecha educativa y una baja alfabetización digital. La oportunidad de mejora también se presenta en las actuales regulaciones de la región, que dictan las normas para

el tratamiento de datos personales digitales.

Como muestra la sección *Panorama regulatorio y normativa de privacidad de datos en Latinoamérica*, cada vez más se actualizan las leyes de privacidad y se le da mayor importancia al tema en la región. Este análisis de los cambios más recientes en estas herramientas demuestra esfuerzos importantes para alinearse con los más altos estándares internacionales. No obstante, también se observa una falta de enfoque en la privacidad de los menores de edad, particularmente en cómo se adaptan estas regulaciones y normativas al ambiente educativo estudiantil.

Basado en este análisis, proveniente de investigación de la literatura, 15 entrevistas con personas expertas en diferentes temáticas relevantes, dos conversatorios con docentes de la región y la Encuesta de Escuelas en Línea Seguras LATAM, en la que participaron alrededor de 1300 docentes, se emitieron 14 recomendaciones divididas en cuatro categorías para fortalecer la protección de los datos digitales de niños y niñas en ámbitos educativos, que ofrecen ejemplos y casos de uso relevantes a lo largo de las explicaciones.

Si bien esta lista termina con la recomendación de crear un modelo escolar nuevo, con suficiente resiliencia para subsistir en un mundo que cada vez tiene más riesgos digitales, también se incluyen acciones de diferentes alcances, que incluyen diferentes tipos de actores para que su implementación pueda empezar sin más espera. Urge garantizar una transición hacia ambientes educativos digitales más seguros para que la pandemia no deje vulnerable a toda una generación, sino que más bien nos sirva de aprendizaje para adelantarnos hoy a la educación del futuro.

Anexos

Anexo 1 - Clasificación de los tipos de datos que podrían recolectarse en plataformas educativas

Nota: esta lista es ilustrativa. No pretende ser exhaustiva y está sujeta a las regulaciones de cada país. Su autoría es del Grupo BID y C Minds.

Datos biométricos⁴⁰

1. Reconocimiento facial.
2. Reconocimiento del iris.
3. Escáner de huellas dactilares.
4. Reconocimiento de la voz.
5. Geometría de la mano.
6. Características del comportamiento.
7. Datos biométricos variables como las pulsaciones de las teclas, la escritura a mano, la forma de caminar, el modo de utilizar el “ratón” y otros movimientos que pueden evaluarse e identificar quién es el estudiante.

Metadatos⁴¹ de la tecnología de aplicaciones

1. Direcciones IP y *cookies*⁴².
2. Estadísticas de uso de la aplicación.
3. Por último, cualquier metadato es aquel que puede definirse como un dato que nace a partir del modo en que los usuarios y visitantes se relacionan con las distintas funciones de una plataforma. Por ejemplo, si hay recursos a los que los docentes acceden repetidamente. Eso puede ser una señal de que ven valor en ellos. Por el contrario, si hay recursos que los docentes no utilizan a menudo, eso podría ser una señal de que hay margen de mejora. Lo mismo ocurre con las interacciones de los estudiantes con los recursos.

40 La biometría es una forma de medir las características físicas de una persona para verificar su identidad. Puede incluir rasgos fisiológicos, como las huellas dactilares y los ojos, o características de comportamiento, como la forma única de completar un rompecabezas de autenticación de seguridad. Aunque pueden variar, aquí se presentan siete de ellos.

41 Los metadatos se definen como los datos que proporcionan información sobre uno o más aspectos de los datos. Es decir, que se derivan de un cálculo de los datos recolectados.

42 Las *cookies* son un pequeño archivo enviado por los sitios web, el cual se almacena en el navegador del usuario y contiene información relacionada con este sobre un sitio web específico. Dentro de sus usos están recordar preferencias, registrar compras y dejar la sesión abierta, entre muchas otras ([Kaspersky](#), s.f.).

Datos de evaluación

1. Datos de pruebas estandarizadas (ENLACE, PISA, o cualquier otra prueba que se aplique en Latinoamérica.)
2. Datos de observación: los docentes la utilizan como otra forma de determinar el progreso de sus estudiantes. Por ejemplo, pueden observar las interacciones de ellos con sus compañeros a través del trabajo en proyectos. El rendimiento de los alumnos en algunos proyectos se evalúa mediante una presentación oral; el profesor puede introducir comentarios y calificaciones a esas presentaciones.
3. Asistencia: escuelas y colegios pueden optar por utilizar esta información para ayudar a controlar las ausencias crónicas, que pueden tener un impacto adverso en el rendimiento estudiantil, como por ejemplo:
 - a. Datos de asistencia escolar (diaria) de los estudiantes.
 - b. Datos de asistencia a clase.
 - c. Otros datos de asistencia: suspensiones/expulsiones.

Datos demográficos

1. Fecha o año de nacimiento.
2. Género.
3. Origen étnico o raza.
4. Información sobre el idioma (idioma materno, preferido o principal que habla el estudiante).
5. Situación socioeconómica.
6. Información financiera sobre la matrícula estudiantil.
7. Grado que cursa el estudiante.
8. Salón de clases al que asiste regularmente.
9. Orientación religiosa de la familia.
10. Domicilio.

Datos curriculares específicos

1. Año de graduación.
2. Correo electrónico.
3. Teléfono.
4. ID del sistema de los padres/tutores.

5. Número de identificación de los padres.
6. Nombre o apellido del padre, madre o tutor.
7. Horario.
8. Cursos programados por el alumno.
9. Indicador especial (como un retraso de pago, falta de devolución de material o inasistencia a un programa extracurricular).
10. Información sobre el nivel de inglés o cualquier otra lengua extranjera de los estudiantes.
11. Ingresos.
12. Información sobre alguna discapacidad del estudiante.

Identificadores de estudiantes

1. Número de identificación local (distrito escolar).
2. Número de identificación estatal.
3. Número de identificación del estudiante asignado por el proveedor o por la aplicación.
4. Rendimiento del estudiante en la aplicación.
5. Desempeño del programa/aplicación (por ejemplo, programa de lectura: el estudiante lee por debajo del nivel esperado del grado).

Pertenencia del estudiante al programa

1. Actividades académicas o extracurriculares a las que un estudiante puede pertenecer o en las que puede participar.
2. Respuestas de los estudiantes a las encuestas.
3. Comprensión de sus pasiones e intereses.

Estas conversaciones son también una parte útil del proceso de planificación para el ingreso a la universidad (por ejemplo, pueden ayudar con su ensayo de solicitud a la universidad).

Trabajo de los estudiantes

1. Contenidos generados por los estudiantes: escritos, imágenes, etc. A lo largo del curso escolar, los estudiantes pueden subir información a una plataforma educativa, por ejemplo, notas sobre su progreso, sus objetivos personales para la semana o sus productos finales para un proyecto en particular.

2. Información sobre los resultados de evaluación de los estudiantes y el expediente académico.
3. Información sobre los resultados de los estudiantes (promoción y matriculación en el grado, información sobre los exámenes generales, resultados de los exámenes de admisión a la universidad, elegibilidad y aceptación en la universidad, y empleo).
4. Calificaciones de los cursos de los estudiantes/notas de rendimiento.

Anexo 2 - Definición de los riesgos⁴³



1. Ciberacoso

El ciberacoso, que 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 que aquellas que los estudiantes podrían hacer en persona. 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.



2. Amenazas por correo electrónico

Cuando personas sin autorización tienen acceso a los correos de estudiantes o si de alguna manera esos correos se hacen públicos (por descuido o por ciberataque a la escuela), es posible que haya hostigamiento o amenazas vía correo electrónico.



3. Flaming

Cuando una persona insulta o agrede a otra en discusiones exageradas o acaloradas en un foro online, puede producirse el *flaming*, que es un acoso e imprecación llevados a un nivel extremo en público. Aunque tener control sobre esto es relativamente sencillo en plataformas escolares, es necesario considerar que este riesgo puede existir en espacios fuera del control de la institución escolar. Este riesgo es más alto si esas instituciones redirigen a los estudiantes a un espacio, medio o plataforma que cuente con una sección de comentarios abiertos al público y donde se puede opinar de manera anónima, por ejemplo cuando se manda como tarea mirar un video de alguna plataforma externa al plantel educativo.



4. Outing

El *outing* es el acto de hacer pública 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 información privada de manera involuntaria.



5. Phishing

El *phishing* es un ciberataque en el que el atacante se hace pasar por una entidad o persona de confianza y, empleando ingeniería social y medios electrónicos falsos, utiliza el correo electrónico como arma para robar datos privados como, por ejemplo, el número de la tarjeta de crédito. El objetivo es engañar al destinatario del correo electrónico para que crea que el mensaje es algo que quiere o necesita. Esto se refiere a que es posible que

⁴³ Esta clasificación proviene de la Guía rápida del proyecto Aprendizaje Seguro en Línea del BID y C Minds, 2021.

una persona se haga pasar por un alumno o docente para poder engañar y entablar una conversación con estudiantes.



6. Acoso por externos

Al tener una fuerte presencia en línea es posible que personas externas a la escuela o colegio puedan tener acceso a comunicaciones con estudiantes y, en consecuencia, los hostiguen. El abuso en línea es cualquier tipo de abuso que ocurre en Internet, facilitado a través de tecnologías como computadoras, tabletas, teléfonos móviles y otros dispositivos con acceso a Internet⁴⁴.



7. Robo de identidad

Por el alcance tratado en este documento el robo de identidad es la creación de un perfil falso o hacerse pasar por otra persona en redes, diciendo cosas vergonzosas, lascivas o malvadas para crear una mala imagen suya en Internet.



8. Malware

El *malware* lo define la OCDE como un *software* malicioso que se inserta en un sistema de información, normalmente en forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, las aplicaciones o el sistema operativo de la víctima, o de molestar o interrumpir de otro modo el sistema de la víctima u otros sistemas ([van Eeten y Bauer, 2008](#)).

44 Este 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.

Anexo 3 - Estado de la conectividad en Latinoamérica

A continuación aparece una tabla que contiene índices relacionados con la conectividad y adopción digital de nueve países de la región, seleccionados como representativos a partir del reporte antes mencionado.

Incluye la estrategia de datos por país, porque en varias ocasiones esta contiene las regulaciones de privacidad y seguridad. Esta representatividad se logra al seleccionar tres países en cada cluster de diverso nivel de conectividad (alto, medio y bajo), establecido por el IICA, BID y Microsoft.

Nivel de conectividad en áreas rurales	País	Índice de adopción digital (Banco Mundial, 2018) ⁴⁵	Índice de disponibilidad de red (Foro Económico mundial, 2019)	Índice de accesibilidad de banda ancha (BID, 2016) ⁴⁶	Estrategia digital (hasta abril de 2021)	Estrategia de datos (hasta abril de 2021)
		Avance de adopción digital entre 0 (peor) y 1 (mejor)	Ranking en relación con 121 países	Valor de desempeño entre 1 (peor) y 8 (mejor)	Existencia	Existencia
Alta	Brasil	.64	59/121	4.85	Sí	Sí
	Chile	.72	42/121	5.15	Sí	Sí
	Colombia	.62	69/121	4.80	Sí	Sí
Media	Argentina	.60	58/121	4.73	Sí	Sí
	México	.52	57/121	4.56	Sí	Sí
	Uruguay	.72	46/121	4.43	Sí	Sí
Baja	Bolivia	.48	N/D	3.33	Sí	Sí
	Perú	.55	77/121	4.29	Sí	Sí
	El Salvador	.50	94/121	3.62	Sí	Sí

Se puede observar en la tabla anterior que la región es dispareja en cuanto a infraestructura digital y conectividad y, como lo señala Marcelo Cabrol, Gerente del Área Social del BID, en el reporte antes mencionado: “si no cerramos [la brecha de conectividad], esa barrera cada vez será más alta y tornará aún más desigual a la región, que ya es la más desigual del mundo”.

45 El índice de adopción digital (DAI por sus siglas en inglés) se creó como parte del Informe sobre el Desarrollo Mundial (2016) para evaluar la difusión mundial de las tecnologías digitales entre los tres segmentos de la economía: empresas, personas y gobierno. Se evalúa a los países entre 0 y 1, donde entre más cerca estén del valor 1, mejor trabajo han hecho en la adopción digital. Más información sobre el índice puede verse en <http://wbqfiles.worldbank.org/documents/dec/digital-adoption-index.html>

46 El índice de desarrollo de banda ancha en América Latina y el Caribe mide la brecha digital en la región a través de la evaluación del desarrollo de la banda ancha de los 26 países pertenecientes al Banco Interamericano de Desarrollo, donde se otorga un rango de valores entre 1 y 8: 1 para el peor desempeño y 8 para el mejor. Véase <https://publications.iadb.org/publications/spanish/document/Informe-anual-del-%C3%8Dndice-de-Desarrollo-de-la-Banda-Ancha-en-Am%C3%A9rica-Latina-y-el-Caribe-IDBA-2016.pdf>

Anexo 4 - Brecha de educación

Como lo señala un reporte del BID, “a pesar de los avances registrados en décadas previas un porcentaje considerable de jóvenes en edad de asistir a la educación definida como obligatoria en cada país no se encontraba matriculado en el sistema educativo desde antes de la llegada de la pandemia” ([Acevedo et al., 2020](#)). Con anterioridad a la pandemia ya existían numerosos desafíos en el ámbito educativo mundial; en 2018 había más de 258 millones de niños y niñas fuera de la escuela.

Con la pandemia, la desigualdad en la oferta de modalidades de aprendizaje durante los cierres de escuelas y colegios probablemente creará desigualdades a largo plazo ([ONU, 2020](#)). En efecto, aproximadamente 23.8 millones de niños, niñas y jóvenes (de preescolar a educación universitaria) pueden abandonar o no tener acceso a la institución educativa el próximo año como resultado del impacto económico de la pandemia ([ONU, 2020](#)).

“El cierre de las escuelas y de otros espacios de aprendizaje ha impactado a 94 % de la población mundial de estudiantes, hasta 99 % en los países de ingresos bajos y medio-bajos” ([ONU, 2020](#)). Frente a este panorama, la incorporación de tecnologías que permitan la educación a distancia no solo es una respuesta de emergencia ante un siniestro mundial, sino un cambio estructural que tiene el potencial de mejorar la educación y la calidad de vida de millones de personas en el mundo.

Bibliografía

Acevedo, Ivonne et al. 2020. Los costos educativos de la crisis sanitaria en América Latina y el Caribe. n.d. : BID. <https://publications.iadb.org/publications/spanish/document/Los-costos-educativos-de-la-crisis-sanitaria-en-America-Latina-y-el-Caribe.pdf>

Álvarez Marinelli, Horacio et al. 2020. La educación en tiempos del coronavirus. BID. <https://publications.iadb.org/publications/spanish/document/La-educacion-en-tiempos-del-coronavirus-Los-sistemas-educativos-de-America-Latina-y-el-Caribe-ante-COVID-19.pdf>

Arias Ortiz, Elena et al. 2021. *Los Sistemas de Información y Gestión Educativa (SIGED) de América Latina y el Caribe: la ruta hacia la transformación digital de la gestión educativa*. BID. <https://publications.iadb.org/publications/spanish/document/Los-Sistemas-de-Informacion-y-Gestion-Educativa-SIGED-de-America-Latina-y-el-Caribe-la-ruta-hacia-la-transformacion-digital-de-la-gestion-educativa.pdf>

Berríos, Soledad. 2013. *Alfabetización digital como política de Estado*. Universidad del Pacífico y Universidad Nacional de Cuyo. <https://www.alfabetizaciondigital.redem.org/wp-content/uploads/2015/07/Alfabetización-digital-como-políticande-Estado.pdf>

BID. 2015. Infraestructura, logística y conectividad: Uniando a las Américas. BID. <https://publications.iadb.org/es/publicacion/15428/infraestructura-logistica-y-conectividad-uniando-las-americas>

BID. 2020b. *Ficha técnica: Plataforma Adaptativa de Matemáticas (PAM)*. <https://fairlac.iadb.org/es/plataforma-adaptativa-matematicas>

Byrne, Jasmina et al. 2021. *The Case for Better Governance of Children's Data: A Manifesto*. UNESCO. https://www.unicef.org/globalinsight/reports/better-governance-childrens-data-manifesto?utm_source=Data+Stewards+Network&utm_campaign=176fee9715-EMAIL_CAMPAIGN_2019_05_17_08_37_COPY_01&utm_medium=email&utm_term=0_bc6d09925f-176fee9715-87848949

CEPAL. 2020. *EDUCATION IN THE TIME OF COVID-19*. ECLAC-UNESCO. https://repositorio.cepal.org/bitstream/handle/11362/45905/1/S2000509_en.pdf

CEPAL-UNESCO. 2020. *La educación en tiempos de la pandemia de COVID-19*. https://repositorio.cepal.org/bitstream/handle/11362/45904/S2000510_es.pdf?sequence=1&isAllowed=y

Cobo, Cristobal et al. 2020. *Cómo utilizan la tecnología los países de América Latina durante el cierre de las escuelas a causa de la COVID-19*. Banco Mundial. <https://blogs.worldbank.org/es/education/como-utilizan-la-tecnologia-los-paises-de-america-latina-durante-el-cierre-de-las>

Cotacachi, David y Grigera, Ana. 2020. *2020 inclusivo: tecnología accesible para los pueblos indígenas*. BID. <https://blogs.iadb.org/igualdad/es/2020-inclusivo-tecnologia-accesible-para-los-pueblos-indigenas/>

GSMA. 2016. Connected Society. *Inclusión digital en América Latina y el Caribe*. https://www.gsma.com/latinamerica/wp-content/uploads/2016/05/report-digital_inclusion-4-ES.pdf

Gómez Mont, Constanza et. al. 2020. *La Inteligencia Artificial al servicio del bien social en América Latina y el Caribe: panorámica regional e instantáneas de doce países*. México: BID. <https://publications.iadb.org/publications/spanish/document/La-inteligencia-artificial-al-servicio-del-bien-social-en-America-Latina-y-el-Caribe-Panorámica-regional-e-instantáneas-de-doce-paises.pdf> Naciones Unidas. 2020. *Policy Brief: Education during COVID-19 and beyond*. n.d.: Naciones Unidas. https://www.un.org/development/desa/dspd/wp-content/uploads/sites/22/2020/08/sg_policy_brief_covid-19_and_education_august_2020.pdf?utm_content=buffer8f0e0&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer

Hernández Armenta, Mauricio. 2020. *Las escuelas de educación básica enfrentan riesgos cibernéticos ante aprendizaje remoto*. México: Forbes. <https://www.forbes.com.mx/las-escuelas-de-educacion-basica-enfrentan-riesgos-ciberneticos-ante-aprendizaje-remoto/>

Jara, Ignacio y Ochoa, Juan Manuel. 2020. *Usos y efectos de la inteligencia artificial en educación*. BID. <https://publications.iadb.org/publications/spanish/document/Usos-y-efectos-de-la-inteligencia-artificial-en-educacion.pdf>

Jaramillo, Carlos Felipe. 2020. *Cerrar la brecha digital para combatir la pobreza en América Latina y el Caribe*. Banco Mundial <https://blogs.worldbank.org/es/latinamerica/cerrar-la-brecha-digital-para-combatir-la-pobreza-en-america-latina-y-el-caribe>

Naciones Unidas. s.f. Noticias de Inteligencia Artificial. Naciones Unidas. <https://news.un.org/en/tags/artificial-intelligence>

Omar, Ortega. 2018. *67% de las escuelas de Latinoamérica han sido víctimas de ciberataques*. México: El Financiero. <https://www.elfinanciero.com.mx/tech/67-por-ciento-de-las-escuelas-de-latinoamerica-han-sido-victimas-de-ciberataques/>

Paykamian, Brandon. 2021. *Report: 'Record-Breaking' Cyber Attacks on Schools in 2020*. Government Technology. <https://www.govtech.com/policy/2020-marks-a-record-breaking-year-for-cyber-attacks-against-schools.html>

Simonite, Tom. 2020. *Meet the Secret Algorithm That's Keeping Students Out of College*. Wired. <https://www.wired.com/story/algorithm-set-students-grades-altered-futures/>

Skelton, Sebastian Klovig. 2021. *Nottinghamshire schools suspend online learning following cyber attack*. Computer Weekly. <https://www.computerweekly.com/news/252497342/Nottinghamshire-schools-suspend-online-learning-following-cyber-attack>

Stoilova, Mariya et al. 2021. *Investigating Risks and Opportunities for Children in a Digital World*. UNICEF, LSE. <https://www.unicef-irc.org/publications/pdf/Investigating-Risks-and-Opportunities-for-Children-in-a-Digital-World.pdf>

Subedi, Sushant. 2020. *The digital divide in education: Policy lessons from the pandemic*. LSE. <https://blogs.lse.ac.uk/socialpolicy/2020/08/26/the-digital-divide-in-education-policy-lessons-from-the-pandemic/>

UNESCO. 2020. *COVID-19: La acción que lleva a cabo la Coalición Mundial para la Educación de la UNESCO ante el mayor trastorno del aprendizaje nunca experimentado*. UNESCO. <https://es.unesco.org/news/covid-19-accion-que-lleva-cabo-coalicion-mundial-educacion-unesco-mayor-trastorno-del>

UNICEF. 2021. *Las escuelas de más de 168 millones de niños del mundo llevan casi un año entero cerradas por completo debido al COVID-19*. Nueva York: unicef. [unicef.org/es/comunicados-prensa/escuelas-168-millones-ninos-llevan-casi-ano-entero-cerradas-debido-covid19](https://www.unicef.org/es/comunicados-prensa/escuelas-168-millones-ninos-llevan-casi-ano-entero-cerradas-debido-covid19)

UNPRI. 2020. *Theme 3: Covid-19, privacy rights and cyber security risks*. <https://www.unpri.org/covid-19-resources/theme-3-covid-19-privacy-rights-and-cyber-security-risks/6343.article>

van Eeten, Michel J.G. y Bauer, Johannes M. 2008. *Economics of malware: security decisions, incentives and externalities*. n.d.: OCDE. <https://www.oecd.org/sti/ieconomy/40722462.pdf>

Waldrop, Theresa. 2020. *Here's what happened when students went to school during the 1918 pandemic*. GMT: CNN. <https://edition.cnn.com/2020/08/19/us/schools-flu-pandemic-1918-trnd/index.html>

Walefield, Jane. 2021. *Malware found on laptops given out by government*. BBC News. <https://www.bbc.com/news/technology-55749959>

Young, Andrew. 2020. *Responsible group data for children*. New York: UNICEF. <https://www.unicef.org/globalinsight/media/1251/file/UNICEF-Global-Insight-DataGov-group-data-issue-brief-2020.pdf>

