La IA y la Ciberseguridad en los ambientes educativos

Karla Patricia Alas de Duarte

La IA y la Ciberseguridad en los ambientes educativos

Karla Patricia Alas de Duarte

GEDA GROUP y Estudio Kapadu

La educación atraviesa un punto de inflexión, un crisol donde la tradición pedagógica se funde con la innovación disruptiva. Aferrarse a educar como antaño, siguiendo los paradigmas de la vieja escuela, es cada vez más un camino insostenible. Las nuevas generaciones portan en su ADN cultural una predisposición innata hacia la tecnología, lo cual explica sus legítimas exigencias de modernización. Por ello, la Academia tiene la imperiosa tarea de mejorar sus formas de enseñanza. Al mismo tiempo, es una verdad incuestionable que la inteligencia artificial (IA) se ha integrado en nuestras aulas, ofreciendo un amplísimo espacio creativo cuyos atributos benefician por igual a docentes y estudiantes (Caballero & Calvo, 2023).

Surgimiento del nuevo concepto: “Ciber IA Educativa”

En el corazón de esta transformación digital emerge un nuevo paradigma: la Ciber IA Educativa. Este concepto, que representa la convergencia estratégica entre la inteligencia artificial y la ciberseguridad aplicada a entornos de aprendizaje, se perfila como una fuerza disruptiva. Su potencial no solo reside en la protección de datos sensibles, sino también en redefinir las distintas metodologías de enseñanza del siglo XXI.

La Ciber IA Educativa no solo impulsa el potencial educativo mediante herramientas innovadoras, adaptadas a estudiantes altamente tecnificados, sino que también subraya

una verdad esencial: la ciberseguridad no puede seguir siendo un aspecto secundario en la educación digital, debe ocupar un lugar central en su ecosistema. Este nuevo enfoque nos permite comprender cómo la sinergia entre la IA y la ciberseguridad genera múltiples oportunidades para enriquecer el aprendizaje y promover entornos más seguros en una sociedad plenamente digitalizada.

> Las instituciones de educación superior necesitan introducir marcos de ciberseguridad impulsados por IA debido a las limitaciones de los sistemas de seguridad convencionales. Esto limitará las amenazas cibernéticas, mejorará la detección de amenazas en tiempo real y los sistemas de respuesta automatizada, y fortalecerá el cumplimiento normativo. (Wada et al., 2025, p. 2234)

Además, ofrece a los docentes herramientas no solo para enseñar con mayor eficacia, sino que protege los datos personales y académicos, de estudiantes, maestros y centros educativos, que hoy se encuentran especialmente expuestos en dichos entornos digitales. La expansión de la inteligencia artificial en la educación exige una reevaluación crítica de la privacidad, el control de datos y la justicia digital, temas que no pueden separarse de la infraestructura educativa actual (Clemente Alcocer et al., 2024). Esta perspectiva respalda la idea de que el concepto de Ciber IA Educativa, es útil y necesario para avanzar hacia una educación más segura, ética y transformadora.

Auge de la Inteligencia Artificial (IA)

Como punto de partida, la IA ha experimentado un notable auge en los ambientes educativos, transformando significativamente los procesos de enseñanza-aprendizaje, y adaptándolo a las necesidades específicas de cada estudiante, así como automatizar tareas administrativas y pedagógicas mediante herramientas, como chatbots educativos, sistemas de tutoría inteligente y plataformas de análisis de datos (Gómez Contreras, 2024).

No obstante, este avance tecnológico, aunque prometedor, ha trazado una línea crítica: el surgimiento de desafíos asociados al uso de la IA en las aulas, especialmente en el ámbito de la ciberseguridad. En la medida en que estas tecnologías se integran en

los entornos educativos, también aumenta la superficie de exposición a ciberataques. Esto hace indispensable fortalecer los mecanismos de protección de datos sensibles de estudiantes y docentes (Luckin et al., 2016).

Amenazas como el phishing, el malware, el robo de identidad, y otras formas de explotación de vulnerabilidades pueden tener consecuencias graves en la infraestructura educativa digital. De ahí que la integración responsable y segura de la IA en la educación, debe contemplar un enfoque basado en la gestión de riesgos y la implementación de políticas robustas de seguridad de la información (Wada et al., 2025).

La IA como aliada en la ciberseguridad

Aunque el panorama digital actual puede parecer desafiante, la IA surge como una herramienta poderosa para contrarrestar los ciberataques. Nos encontramos en una era en la que los algoritmos de aprendizaje automático, son capaces de detectar anomalías y patrones sospechosos en tiempo real, elevando así la capacidad de defensa digital en los entornos más críticos.

> Técnicas populares de IA como el Aprendizaje Automático (ML), el Aprendizaje Profundo (DL), el Procesamiento del Lenguaje Natural (NLP) y el modelado de Sistemas Expertos (ES) basados en conocimiento o reglas pueden usarse para mitigar problemas de ciberseguridad. Las técnicas basadas en aprendizaje automático, especialmente el aprendizaje profundo, se han destacado por su capacidad para detectar amenazas de manera temprana. (Wada et al., 2025, p. 2234)

Una de las principales ventajas de la IA, en materia de ciberseguridad radica en su capacidad para automatizar tareas de protección, como la detección de intrusiones, la gestión de vulnerabilidades y la respuesta a incidentes. Este enfoque no solo mejora la eficiencia operativa, sino que también permite una reacción proactiva y en tiempo real ante amenazas emergentes (Buczak & Guven, 2016).

En un mundo cada vez más digitalizado, la ciberseguridad se ha convertido en una prioridad para individuos, empresas y gobiernos. La creciente sofisticación de los

ciberataques demanda soluciones inteligentes y escalables, y en este contexto, la IA se posiciona como una aliada estratégica (Kaur et al., 2023). Entre sus principales aportes se destacan:

- La detección temprana de amenazas a través del análisis masivo de datos, para identificar patrones anómalos que podrían indicar actividades maliciosas.
- El aprendizaje de ataques anteriores para reconocer nuevas variantes, incluso ataques de día cero.
- La automatización de respuestas ante incidentes, como el aislamiento de dispositivos infectados, el bloqueo de tráfico malicioso y la aplicación inmediata de parches.
- El análisis de comportamiento de usuarios (User Behavior Analytics), que permite identificar accesos inusuales, movimientos laterales en la red o intentos de exfiltración de datos.
- La implementación de mecanismos de autenticación biométrica (como el reconocimiento facial y de voz) que fortalecen el control de acceso a sistemas críticos.

Asimismo, podemos constatar con Kaur et al. (2023), que la inteligencia artificial no solo está redefiniendo los paradigmas de la ciberseguridad, sino que, a su vez, es moldeada y retada constantemente por las necesidades cada vez más sofisticadas y críticas de este campo en evolución. Este ciclo de retroalimentación mutua (la IA fortalece las defensas y las nuevas amenazas, a su vez, perfeccionan los algoritmos) cristaliza una verdadera simbiosis tecnológica. Lejos de ser una mera herramienta reactiva, esta sinergia establece los cimientos para un nuevo ecosistema de defensa digital intrínsecamente robusto, capaz de resistir ataques de alto calibre; adaptativo, que aprende y evoluciona en tiempo real frente a tácticas novedosas; y predictivo, con la capacidad de anticipar vulnerabilidades y neutralizar amenazas potenciales antes de que se materialicen. Así, se configura un escenario donde la protección deja de ser un escudo estático para convertirse en un ente proactivo (Wiafe et al., 2020).

Implementación estratégica de la “Ciber IA” en los centros educativos

Para que la IA evolucione hacia su máximo potencial como Ciber IA Educativa (es decir, como una aliada estratégica en la defensa digital de los centros educativos) es primordial integrar herramientas de ciberseguridad con tecnologías inteligentes de forma estratégica y planificada. Las técnicas de IA, en particular el aprendizaje automático y el aprendizaje profundo, muestran resultados prometedores para mejorar las soluciones de ciberseguridad al detectar y mitigar amenazas en evolución (Zeadally et al., 2020).

La Ciber IA Educativa no debe concebirse como una solución improvisada o meramente tecnológica, sino como el resultado de un proceso de adecuación institucional, donde confluyen: la innovación pedagógica, la gestión proactiva de riesgos, la alfabetización digital avanzada y una cultura institucional sólida en torno a la protección de datos. Todo ello debe sustentarse en un modelo de implementación estructurado, cimentado sobre tres pilares: Diagnóstico del entorno digital educativo, Plan de adecuación y fortalecimiento de la ciberseguridad con IA, y Capacitación del personal y gobernanza digital (Tabla 1).

Tabla 1. Pilares de la Ciber IA Educativa

Diagnóstico del entorno digital educativo	Plan de adecuación y fortalecimiento de la ciberseguridad con IA	Capacitación del personal y gobernanza digital
Evaluar el estado actual de los sistemas tecnológicos del centro educativo, identificando vulnerabilidades, recursos disponibles y nivel de madurez digital de docentes y estudiantes.	Incorporar soluciones inteligentes como: • Plataformas de monitoreo con IA en tiempo real. • Herramientas de detección automática de amenazas. • Sistemas biométricos de autenticación para accesos críticos. • Protocolos automatizados de respuesta ante incidentes. • Este plan debe contemplar la actualización constante de algoritmos y políticas de protección de datos.	Formar a docentes, administradores y estudiantes en: • Ciber higiene, • Ética digital y • Uso seguro de herramientas con IA. • Establecer un comité de gobernanza tecnológica que supervise la correcta ejecución del plan.

Fuente: elaboración propia.

De este modo, la Ciber IA Educativa se erige como ese “héroe sin capa” que opera de forma proactiva y silenciosa desde las infraestructuras digitales. Su labor es garantizar la integridad de los sistemas, salvaguardar la privacidad de los datos y asegurar la continuidad del proceso de aprendizaje. Así, trasciende de ser una mera tendencia tecnológica para consolidarse como una evolución necesaria e imprescindible, constituyendo la barrera más eficaz frente a las crecientes y sofisticadas amenazas que acechan el ciberespacio educativo (Brundage et al, 2018).

Implementación de herramientas de ciberseguridad con IA en centros educativos

A continuación, se presenta una propuesta sobre ciertos pasos para implementar herramientas de ciberseguridad con IA en centros educativos:

Paso 1: creación de un plan de adecuación. Cuando se involucra herramienta de IA y Ciberseguridad en centros educativos, debemos partir de un análisis de riesgos, que nos permita identificar las vulnerabilidades específicas, como el acceso no autorizado a datos de estudiantes, ataques de phishing dirigidos a profesores, o el uso indebido de dispositivos conectados y así poder evaluar el impacto potencial de estos riesgos.

Paso 2: identificar metas para la planificación. Establecer metas claras para la implementación de la ciberseguridad con IA, como la detección temprana de amenazas, la automatización de respuestas a incidentes, o la mejora de la concienciación sobre seguridad.

Paso 3: elección de las herramientas. Para ello se debe investigar y elegir soluciones de ciberseguridad que incorporen IA, como sistemas de detección de intrusiones y sistemas de información y gestión de eventos de seguridad basados en IA, así como asegurarse de que las herramientas sean compatibles con la infraestructura existente y escalables para el futuro.

Paso 4: configuración e integración de datos. Esto implica el conectar las herramientas de IA, a diversas fuentes de datos, como registros de red, registros de usuarios y datos de comportamiento, para obtener una visión completa del entorno de seguridad.

Paso 5: entrenamiento de la IA. Con esto se pretende ajustar los parámetros de la IA para optimizar la precisión y reducir los falsos positivos y alimentar a los algoritmos de IA con datos de alta calidad y relevantes para que puedan aprender a identificar patrones de comportamiento malicioso.

Paso 6: automatización de respuestas. Se puede configurar las herramientas de IA para que automaticen las respuestas a incidentes comunes, como el bloqueo de direcciones IP maliciosas o el aislamiento de dispositivos infectados así también como establecer protocolos claros para la intervención humana en caso de incidentes complejos.

Herramientas y tecnologías

Algunas herramientas tecnológicas que pueden implementarse en los ambientes educativos con la integración de Ciber IA son:

- Sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS) basados en IA: para detectar y bloquear actividades maliciosas en la red.
- Plataformas de inteligencia de amenazas (TIP) con IA: para recopilar y analizar información sobre amenazas cibernéticas y anticipar posibles ataques.
- Herramientas de análisis de comportamiento del usuario (UBA) con IA: para detectar actividades sospechosas basadas en patrones de comportamiento inusuales.
- Soluciones de seguridad de endpoints (EDR) con IA: para proteger los dispositivos de los usuarios contra malware y otras amenazas.

Al implementar estas estrategias y herramientas, los centros educativos pueden aprovechar el poder de la IA para fortalecer su ciberseguridad y crear un entorno digital más seguro para todos.

Valores a considerar en una estrategia de ciber IA, en el entorno educativo

Podemos identificar por medio de la siguiente matriz, los siguientes valores a considerar en una estrategia de Ciber IA en el entorno educativo:

Tabla 2. Matriz de valores para la Ciber IA Educativa

Activo con IA	Subtemas Relevantes	Amenaza	Evaluación del Riesgo (Impacto / Probabilidad)	Nivel de Prioridad	Medidas de Mitigación
Sistemas de Aprendizaje Adaptativo con IA	• Plataformas que personalizan contenidos. • Sistemas de recomendación de tareas. • Evaluaciones automatizadas	Manipulación de algoritmos Fuga de datos personales del alumno	Alto / Medio	Alta	• Validación de integridad del sistema. • Evaluaciones externas del modelo IA. • Cifrado y anonimización de datos.
Chatbots Educativos / Asistentes Virtuales	• Chatbots en páginas web. • Asistentes para preguntas frecuentes. • Soporte automatizado.	Inyección de comandos maliciosos Suplantación de identidad	Alto / Medio	Alta	• Entrenamiento seguro del modelo. • Filtrado de entrada/salida. • Registro de interacciones y monitoreo.
Análisis de Comportamiento Estudiantil con IA	• Seguimiento de rendimiento. • Detección de abandono escolar. • Análisis predictivo.	Uso indebido de datos sensibles Discriminación algorítmica	Muy alto / Medio	Muy alta	• - Transparencia algorítmica. - Revisión humana de decisiones críticas. - Evaluaciones éticas de sesgos.

Activo con IA	Subtemas Relevantes	Amenaza	Evaluación del Riesgo (Impacto / Probabilidad)	Nivel de Prioridad	Medidas de Mitigación
Cámaras con Reconocimiento Facial	• Control de acceso. • Registro de asistencia. • Seguridad perimetral.	Uso indebido de imágenes Violación de privacidad	Muy alto / Alto	Muy alta	• Consentimiento explícito informado. • Almacenamiento seguro de imágenes. • Auditorías de uso de biometría.
IA en Sistemas de Detección de Intrusos (IDS/ IPS)	• IA que identifica patrones anómalos. • Respuesta automática a amenazas	Falsos positivos/ negativos Fallos en detección de amenazas reales	Medio / Medio	Media	• Entrenamiento constante del sistema. • Supervisión humana complementaria. • Actualizaciones regulares.
Herramientas de IA Generativa en el Aula	• Generadores de texto. • Creadores de imágenes y presentaciones. • Traducción automática	Generación de contenido inapropiado Fuga de información ingresada	Alto / Medio	Alta	• Filtros de contenido. • Política de uso claro para estudiantes. • Control de entradas sensibles
Plataformas de Evaluación Automatizada con IA	• Corrección automática de pruebas. • Análisis semántico de respuestas.	Manipulación del sistema de calificación Fallos en equidad del modelo	Alto / Alto	Muy alta	• Revisión humana obligatoria en evaluaciones críticas. • Validación del algoritmo por docentes. • Transparencia en criterios de corrección.

Activo con IA	Subtemas Relevantes	Amenaza	Evaluación del Riesgo (Impacto / Probabilidad)	Nivel de Prioridad	Medidas de Mitigación
Bases de Datos de Entrenamiento IA	• Datos recopilados para entrenar modelos. • Información académica e institucional.	Recolección excesiva / sin consentimiento Filtración de datasets sensibles	Muy alto / Medio	Muy alta	• Gobernanza de datos. • Anonimización y reducción de datos. • Políticas claras de recolección y uso

Fuente: elaboración propia.

Privacidad o intrusión: el dilema de las herramientas de ciberseguridad con IA en centros educativos

Hasta aquí, hemos analizado la conveniencia de la alianza que propone la Ciber IA Educativa, demostrando cómo la adopción de herramientas de inteligencia artificial puede reforzar la seguridad, optimizar los procesos administrativos y personalizar el aprendizaje (Wang et al., 2024). Sin embargo, este panorama prometedor inevitablemente plantea interrogantes: ¿Estamos protegiendo a los estudiantes o estamos invadiendo su privacidad? Y ¿Cómo estamos protegiendo la infraestructura de los centros educativos, y la información que éstos manejan?

No podemos negarnos a que la evolución tecnológica nos abrace, eso sería retroceder en una era como la que estamos viviendo, y siendo esta alianza, como gran promesa en la ciberseguridad educativa, así como en el uso de IA en los entornos escolares. Su avance seguirá creciendo exponencialmente, y una opción viable es prepararnos y fortalecernos para integrarla de manera responsable.

El que un centro educativo emplee como método de enseñanza las tecnologías, es una gran solución, pero es entendible que, al implementar herramientas o soluciones como sistemas de reconocimiento facial, análisis de comportamiento, plataformas adaptativas y chatbot educativos, que al tiempo que están transformando la experiencia escolar, pueda causar alguna incomodidad por desconocimiento, y muchos piensen que se está afectando a la privacidad (Kamalov et al., 2023).

En el ámbito específico de la ciberseguridad, la inteligencia artificial permite detectar amenazas en tiempo real, prevenir accesos no autorizados y analizar patrones de comportamiento para anticipar ciberataques. Sin embargo, se debe reconocer que estas capacidades no están exentas de riesgos inherentes y conllevan costos asociados significativos que deben ser considerados (Chen et al., 2020).

Riesgos de intrusión a la privacidad

A pesar del beneficio que la IA brinda, puede que estén sucediendo eventos que requieran la atención en el marco de la privacidad (Sadiku et al., 2020), y por lo tanto es importante estar atentos en los siguientes aspectos:

La introducción de cámaras inteligentes y sensores en los centros educativos. Si bien a menudo se justifica bajo la premisa de aumentar la seguridad y prevenir incidentes, inevitablemente plantea la cuestión de una vigilancia potencialmente excesiva. Aunque la intención declarada sea noble, buscando proteger a la comunidad educativa, la implementación generalizada de estos dispositivos puede, paradójicamente, sembrar un clima de desconfianza palpable entre estudiantes, profesores e incluso padres. “La aplicación de la IA en la ciberseguridad presenta considerables problemas éticos y de privacidad. Los sistemas de IA necesitan datos extensos para funcionar efectivamente, lo que provoca aprensiones respecto a la vigilancia y la explotación potencial” (Wada et al., 2025, p. 2235).

Esta sensación de estar constantemente bajo observación puede tener efectos psicológicos significativos. Los estudiantes, en particular, podrían sentir coartada su libertad de expresión y experimentar una presión adicional al saberse permanentemente registrados. Este ambiente de hipervigilancia podría inhibir comportamientos naturales, la espontaneidad y la capacidad de los jóvenes para aprender de sus errores en un entorno que debería fomentar la exploración y el crecimiento personal.

Es especialmente relevante considerar cómo la percepción individual juega un papel primordial en esta dinámica. Algunos usuarios del sistema educativo, ya sea por experiencias previas, rasgos de personalidad o simplemente una mayor conciencia de las implicaciones de la recopilación de datos, pueden ser particularmente sensibles o

sentirse altamente vulnerados ante la presencia constante de tecnologías de control. Lo que para algunos podría parecer una medida de seguridad razonable, para otros podría interpretarse como una invasión de la privacidad y una señal de falta de confianza inherente por parte de la institución educativa.

Esta susceptibilidad puede llevar a reacciones que algunos podrían considerar «alarmistas» ante la implementación de mecanismos de control que el centro educativo percibe como parte integral de la malla curricular o de sus protocolos de seguridad. Sin embargo, estas reacciones no deben descartarse a la ligera. Reflejan una preocupación legítima sobre los límites de la supervisión, el manejo de los datos recopilados y el potencial de que esta información se utilice de maneras imprevistas o que vulneren aún más la privacidad individual.

La clave para mitigar estos riesgos radica en la transparencia, la comunicación clara y la participación de la comunidad educativa en la toma de decisiones sobre la implementación de estas tecnologías. Es imprescindible que los centros educativos expliquen detalladamente los objetivos de la vigilancia, los protocolos de acceso y almacenamiento de los datos, y las garantías existentes para proteger la privacidad de todos. Fomentar un diálogo abierto puede ayudar a construir confianza y a asegurar que las medidas de seguridad no se perciban como una forma de control opresiva, sino como un esfuerzo colaborativo para crear un entorno de aprendizaje seguro y respetuoso para todos.

Plataformas de comportamiento. Para muchas personas, la idea de que un centro educativo implemente sistemas digitales capaces de rastrear el progreso individual de cada alumno e incluso identificar patrones inusuales o “anomalías” genera una comprensible suspicacia. Esta preocupación se centra en el potencial de que los datos recopilados sean utilizados para generar juicios automatizados sobre el desempeño, las capacidades o incluso el comportamiento de los estudiantes.

Una de las principales objeciones radica en el temor de que estos juicios automatizados carezcan de la comprensión y el contexto individual que un educador humano puede ofrecer. Los algoritmos, por sofisticados que sean, se basan en datos predefinidos y pueden no ser capaces de capturar la complejidad de los procesos de aprendizaje, las circunstancias personales que puedan influir en el rendimiento de un estudiante o las diversas formas en que la inteligencia y el talento pueden manifestarse.

Esta falta de comprensión contextual podría llevar a evaluaciones injustas o incompletas, afectando directamente la equidad dentro del sistema educativo. Por ejemplo, un estudiante que aprende a un ritmo diferente o que tiene un estilo de aprendizaje no convencional podría ser etiquetado erróneamente como "anómalo" o con bajo progreso, lo que podría tener consecuencias negativas en sus oportunidades académicas y su autopercepción.

Además, la implementación de sistemas de monitoreo digital plantea interrogantes importantes sobre la libertad de los estudiantes. La sensación constante de ser observado y evaluado por un sistema automatizado podría generar una presión indebida, inhibir la experimentación y la toma de riesgos inherentes al proceso de aprendizaje, y fomentar una cultura de conformidad en lugar de la exploración individual.

La transparencia en el funcionamiento de estas plataformas y en el uso que se da a los datos recopilados se vuelve crucial. Sin una clara rendición de cuentas y mecanismos de supervisión, existe el riesgo de que los juicios automatizados se conviertan en cajas negras, perpetuando sesgos existentes o introduciendo nuevos, sin que los estudiantes o los educadores tengan la capacidad de comprender o cuestionar las decisiones tomadas en base a estos sistemas.

En última instancia, la cuestión de la coexistencia de plataformas de monitoreo en la educación nos invita a reflexionar sobre el equilibrio entre el potencial de la tecnología para mejorar el aprendizaje y la necesidad de proteger la equidad, la libertad y la individualidad de cada estudiante dentro del ecosistema educativo. Es imprescindible un debate continuo y una cuidadosa consideración ética antes de la adopción generalizada de sistemas que puedan tener un impacto tan significativo en la vida académica de los jóvenes.

Bases de datos sensibles. Los modelos de IA requieren grandes volúmenes de datos y por ello, la recolección sin límites o sin el consentimiento adecuado puede vulnerar derechos fundamentales de los menores y jóvenes.

Sesgos algorítmicos. Si los sistemas no son auditados correctamente, podrían replicar sesgos y afectar a ciertos grupos por razones socioeconómicas, culturales o académicas.

Marco jurídico y obligaciones institucionales. La dimensión del marco jurídico y las obligaciones institucionales, son pilares al considerar la implementación de tecnologías

como la inteligencia artificial en el ámbito educativo. La protección de los datos personales no es solo una cuestión ética, sino también un imperativo legal que debe alinearse con las normativas tanto a nivel local como internacional.

Responsabilidades y obligaciones. En este contexto legal, los centros educativos asumen una serie de responsabilidades ineludibles al incorporar herramientas de IA que inevitablemente procesan datos personales de estudiantes, padres y personal. Entre estas obligaciones, destacan:

a. Obtención de consentimiento informado: este es un principio esencial. Antes de recopilar y utilizar datos personales, las instituciones deben obtener un consentimiento explícito, informado y específico. Para los menores de edad, este consentimiento generalmente debe provenir de sus padres o tutores legales. Para los estudiantes mayores de edad, el consentimiento debe ser otorgado por ellos mismos, asegurándose de que comprenden claramente qué datos se recopilarán, con qué fines y cómo se utilizarán.

b. Implementación de evaluaciones de impacto en protección de datos, al usar IA: la introducción de la IA en los procesos educativos conlleva riesgos específicos para la privacidad. Por ello, es decisivo realizarlas antes de la implementación. Estas evaluaciones permiten identificar y analizar los posibles riesgos para la protección de datos que la IA podría generar, así como definir las medidas necesarias para mitigar estos riesgos y garantizar un tratamiento de datos seguro y respetuoso.

c. Aplicación de principios de minimización y transparencia: la recopilación de datos debe limitarse estrictamente a lo necesario para los fines específicos para los que se utilizan. El principio de minimización exige evitar la acumulación innecesaria de información personal. Paralelamente, la transparencia es esencial. Los centros educativos deben informar de manera clara y accesible sobre qué datos se recopilan, cómo se utilizan, quién tiene acceso a ellos y durante cuánto tiempo se conservarán.

d. Establecimiento de protocolos ante filtraciones o mal uso de los sistemas de IA: a pesar de las medidas de seguridad implementadas, siempre existe el

riesgo de incidentes como filtraciones de datos o un uso indebido de los sistemas de IA. Por lo tanto, es elemental contar con protocolos de actuación bien definidos. Estos protocolos deben especificar los pasos a seguir en caso de una brecha de seguridad, incluyendo la notificación a las autoridades competentes y a los afectados, así como las medidas correctivas para contener el incidente y prevenir futuras ocurrencias.

e. Visión ética y coexistencia armoniosa: la visión de una implementación ética y segura de la IA en la educación es substancial, y, la ciberseguridad y la privacidad no deben ser vistas como antagonistas, sino como pilares interdependientes de un mismo objetivo: proteger a la comunidad educativa y sus derechos fundamentales en el entorno digital. La clave para lograr esta coexistencia armoniosa radica en un enfoque proactivo y consciente desde las etapas iniciales de diseño e implementación de cualquier herramienta de IA en el ámbito educativo.

En el caso específico de El Salvador, la Ley de Datos Personales establece el marco legal que las instituciones educativas deben cumplir en esta materia (Ley para la Protección de Datos Personales, 2024; Ley de Fomento a Inteligencia Artificial y Tecnologías, 2025). Es imperativo que los centros educativos salvadoreños se aseguren de que sus prácticas de recopilación y tratamiento de datos se ajusten estrictamente a las disposiciones de esta ley. Y de igual forma esta misma obligatoriedad, rige para la mayoría de países donde está cobrando relevancia este tema.

Aunque las legislaciones específicas puedan variar de un país a otro, existen estándares internacionales, normas técnicas y buenas prácticas en materia de protección de datos que deberían ser consideradas como un umbral mínimo por cualquier institución educativa que maneje información personal. Adoptar estos estándares no solo facilita el cumplimiento normativo, sino que también demuestra un compromiso genuino con la privacidad y la seguridad de los datos de la comunidad educativa, fortaleciendo la confianza en el uso de las tecnologías en el aprendizaje.

Estrategias esenciales

Las estrategias son esenciales para construir un ecosistema tecnológico que priorice la ética y la seguridad (Sadiku et al., 2020). De esta manera se señalan los siguientes puntos:

a. *Diseñar con enfoque ético y legal desde el inicio (Privacy by Design): i*mplica integrar consideraciones de privacidad y seguridad en cada etapa del desarrollo y la implementación de las tecnologías de IA.

En lugar de abordar la privacidad y la seguridad como añadidos posteriores, se deben incorporar como requisitos principales desde la concepción misma de la herramienta.

Esto significa diseñar sistemas que minimicen la recopilación de datos, anonimicen la información siempre que sea posible, ofrezcan transparencia en el procesamiento de datos y permitan a los usuarios tener control sobre su información personal. Al adoptar una filosofía de "Privacy by Design", las instituciones educativas pueden construir sistemas inherentemente más seguros y respetuosos con la privacidad.

b. *Capacitación a docentes y personal técnico en el uso seguro y responsable de la IA***:** a tecnología por sí sola no garantiza la seguridad ni la ética. El factor humano juega un papel determinante. Es imprescindible invertir en la formación integral de los docentes y el personal técnico en relación con las herramientas de IA.

Este tipo de capacitación debe abarcar no solo el funcionamiento técnico de las plataformas, sino también los principios éticos que deben guiar su uso, las mejores prácticas en ciberseguridad para proteger los datos de los estudiantes y los procedimientos para responder ante posibles incidentes de seguridad o violaciones de la privacidad.

Un personal bien informado y consciente de sus responsabilidades es la primera línea de defensa para garantizar un uso seguro y ético de la IA en la educación.

c. *Evaluar constantemente los efectos reales de estas tecnologías en el aula:* La implementación de la IA en la educación no debe ser un proceso estático. Es

esencial establecer mecanismos de evaluación continua para comprender los efectos reales de estas tecnologías en el entorno de aprendizaje.

Esta evaluación debe ir más allá de la mera eficiencia operativa y analizar el impacto en la equidad, la inclusión, la privacidad de los estudiantes, la dinámica de la clase y los resultados del aprendizaje. Los resultados de estas evaluaciones deben utilizarse para realizar ajustes, corregir posibles efectos no deseados y asegurar que la tecnología esté sirviendo verdaderamente a los mejores intereses de la comunidad educativa.

Esta retroalimentación constante permite una adaptación ágil y responsable de las herramientas de IA en el contexto educativo. Al adoptar estas estrategias de manera integral, las instituciones educativas pueden avanzar hacia una implementación de la inteligencia artificial que no solo aproveche su potencial para mejorar la enseñanza y el aprendizaje, sino que también proteja de manera efectiva los derechos y la seguridad de todos los miembros de la comunidad educativa (Crompton & Burke, 2023).

Conclusión

La Ciber IA se convierte en una fuerza dinámica que irrumpe en el panorama educativo con una energía renovadora. Y las 3 “R” son los pilares sobre los que se asienta esta transformación:

Rebelión: La Ciber IA educativa se alza como una rebelión contra las limitaciones de los modelos pedagógicos tradicionales. Al habilitar plataformas de aprendizaje adaptativo, rompe con la rigidez de un currículo único para todos. Cada estudiante se convierte en el centro de su propio viaje educativo, con contenidos y ritmos que se ajustan a sus necesidades y progresos individuales. Esta rebelión personalizada desafía la noción de una educación estandarizada, abriendo paso a experiencias de aprendizaje mucho más significativas y efectivas. Comprende las fortalezas y debilidades de cada alumno, ofreciendo el apoyo y los desafíos precisos en el momento oportuno.

Revolución: se concibe y se experimenta en el aprendizaje. Las simulaciones inmersivas, potenciadas por la inteligencia artificial, transportan a los estudiantes a entornos

virtuales donde pueden explorar conceptos abstractos de manera práctica y vivencial. Desde diseccionar virtualmente un corazón hasta participar en simulaciones históricas interactivas, la revolución inmersiva derriba las barreras del aula física y expande las posibilidades de la exploración y el descubrimiento. Esta transformación va más allá de la mera visualización; implica una interacción profunda y multisensorial que enriquece la comprensión y la retención del conocimiento de formas antes inimaginables.

Resiliencia: en el desafiante mundo digital, la Ciber IA educativa, fortalece la resiliencia humana. Los sistemas de detección de intrusiones, impulsados por la inteligencia artificial y la ciberseguridad, actúan como guardianes vigilantes del ecosistema educativo digital. Protegen la integridad de los datos, la seguridad de las plataformas y la continuidad de las experiencias de aprendizaje en línea. Esta resiliencia no solo se trata de prevenir ataques, sino también de construir sistemas robustos capaces de recuperarse rápidamente ante cualquier eventualidad, asegurando que el proceso educativo no se vea interrumpido por las amenazas cibernéticas.

Este nuevo paradigma educativo puede concebirse como el surgimiento de un Ave Fénix digital. Se trata de un ecosistema de aprendizaje que, fortalecido por la sinergia entre la inteligencia artificial y la ciberseguridad, emerge de las cenizas de los modelos tradicionales portando un escudo protector más robusto e inteligente. Dicho escudo trasciende la mera protección técnica, se erige como un pilar de confianza institucional. Garantiza la soberanía de los datos y la inviolabilidad de la privacidad, pero su valor más profundo radica en generar la tranquilidad indispensable que permite a educadores y estudiantes sumergirse en las posibilidades del mundo digital para colaborar, crear y aprender sin el temor constante.

Por ello, la Ciber IA Educativa no representa una simple evolución tecnológica, sino una metamorfosis radical de la pedagogía misma. Reconfigura los roles, rediseña los espacios de interacción y replantea los objetivos del proceso educativo desde sus cimientos. El futuro que vislumbra es uno donde el aprendizaje es profundamente personalizado, genuinamente inmersivo e intrínsecamente seguro. La “magia” de este paradigma no reside en artilugios tecnológicos, sino en su capacidad para transformar los desafíos más apremiantes del mundo digital (desde la ciberdelincuencia hasta la desinformación) en

oportunidades concretas para construir un aprendizaje no solo más eficaz, sino también más crítico, ético y resiliente. He ahí la verdadera promesa del renacimiento de este paradigma educativo.

Declaración de uso de IA: Se utilizó IA para la conceptualización y organización esquemática de este Capítulo, mediante las plataformas DeepSeek (Inc., 2025, DeepSeek-V3.1) y Consensus (2024, AI-powered research search engine) para validar posibilidades de instrucción en el marco de lo descrito.
Su uso fue mediado por seres humanos.

Referencias

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B., Anderson, H., Roff, H., Allen, G. C., Steinhardt, J., Flynn, C., Ó-hÉigeartaigh, S., Beard, S., Belfield, H., Farquhar, S., ... & Amodei, D. (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. Future of Humanity Institute*. https://arxiv.org/abs/1802.07228

Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502

Caballero, J. & Calvo, D. (2023). Inteligencia artificial y educación: Retos éticos y sociales. *Revista Iberoamericana de Educación*, *91*(1), 45-61. https://doi.org/10.35362/rie9115597

Chen, L., Chen, P., & Lin, Z. (2020). Artificial Intelligence in Education: A Review. *IEEE Access*, *8*, 75264-75278. https://doi.org/10.1109/ACCESS.2020.2988510

Clemente Alcocer, A. A., Cabello Cabrera, A., & Añorve García, E. (2024). La inteligencia artificial en la educación: desafíos éticos y perspectivas hacia una nueva enseñanza. *LATAM Revista Latinoamericana De Ciencias Sociales Y Humanidades*, *5*(6), 464-472. https://doi.org/10.56712/latam.v5i6.3019

Crompton, H., & Burke, D. (2023). Artificial intelligence in higher education: the state of the field. *International Journal of Educational Technology in Higher Education*, *20*, 1-22. https://doi.org/10.1186/s41239-023-00392-8

Decreto Legislativo N.° 144 de 2024. Ley para la Protección de Datos Personales. 15 de noviembre de 2024. D. O. N° 219, Tomo N° 445.

Decreto Legislativo N.° 363 de 2025. Ley de Fomento a Inteligencia Artificial y Tecnologías. 18 de julio de 2025. D. O. N° 134, Tomo N° 448.

Gómez Contreras, F. A. (2024). La tecnología de la palabra y la IA: Una frontera en movimiento. En R. Salazar-Márquez & K. K. Ruiz Mendoza (Eds.), *La tarea en tiempos de la Inteligencia Artificial* (pp. 39-55). IHCC Publicaciones. https://www.doi.org/10.61480/UMEP4135

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

Kamalov, F., Calonge, D., & Gurrib, I. (2023). New Era of Artificial Intelligence in Education: Towards a Sustainable Multifaceted Revolution. *Sustainability*, *15*, 12451. https://doi.org/10.3390/su151612451

Luckin, R., Holmes, W., Griffiths, M. & Forcier, L. B. (2016). *Intelligence Unleashed. An argument for AI in Education*. Pearson. https://www.pearson.com/content/dam/one-dot-com/one-dot-com/global/Files/about-pearson/innovation/open-ideas/IntelligenceUnleashedSPANISH.pdf

Sadiku, M., Fagbohungbe, O., & Musa, S. (2020). Artificial Intelligence in Cyber Security. *International Journal of Engineering Research and Advanced Technology*, *6*(5), 1-7. https://doi.org/10.31695/IJERAT.2020.3612

Wada, I. U., Izibili, G. O., Babayemi, T., Abdulkareem, A., Macaulay, O. M., & Emadoye, A. (2025). AI-driven cybersecurity in higher education: A systematic review and model evaluation for enhanced threat detection and incident response. *World Journal of Advanced Research and Reviews*, *25*(3), 2233–2245. https://doi.org/10.30574/wjarr.2025.25.3.0989

Wang, S., Wang, F., Zhu, Z., Wang, J., Tran, T., & Du, Z. (2024). Artificial intelligence in education: A systematic literature review. *Expert Syst. Appl.*, *252,* 124167. https://doi.org/10.1016/j.eswa.2024.124167

Wiafe, I., Koranteng, F., Obeng, E., Assyne, N., Wiafe, A., & Gulliver, S. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *IEEE Access*, *8*, 146598-146612. https://doi.org/10.1109/ACCESS.2020.3013145

Zeadally, S., Adi, E., Baig, Z., & Khan, I. (2020). Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. *IEEE Access*, *8*, 23817-23837. https://doi.org/10.1109/ACCESS.2020.2968045

Karla Patricia Alas de Duarte

GEDA GROUP y Estudio Kapadu

estudiokpae@gmail.com

https://orcid.org/0009-0003-7116-0220

Karla Patricia Alas de Duarte es una abogada con amplia experiencia en las áreas de nuevas tecnologías, ciberseguridad, y derecho corporativo y mercantil. Socia en dos firmas: GEDA GROUP y Estudio Kapadu. Es miembro activa de Womcy (Women in cybersecurity), Legal Hackers El Salvador e Internet Society (ISOC). Catedrática en diversas universidades del país. En su carrera, ha manejado litigios y asesoría legal en diversas áreas, destacándose en: Tecnologías y Ciberseguridad, casos relacionados con nuevas tecnologías, protección de datos, cibercrimen y ciberseguridad; Litigio y Derecho Mercantil; Asesoría regulatoria ante la Superintendencia de Competencia, la Defensoría del Consumidor y la Superintendencia General de Electricidad y Telecomunicaciones (SIGET). Además, participó en la mesa de redacción de la Ley de Delitos Informáticos y Conexos en la Asamblea Legislativa de El Salvador.