

Día del internet seguro: Seguridad Digital para Educar en tiempos de IA

2026-02-09

Día del internet seguro: Seguridad Digital para Educar en tiempos de IA

El 10 de febrero de 2026 la comunidad educativa global conmemorará una nueva edición del Día Internacional de Internet Seguro, una iniciativa impulsada por el Instituto Nacional de Ciberseguridad (INCIBE) y la Unión Europea. Bajo el lema "Seguridad Digital para Educar en tiempos de IA", este año el foco se desplaza hacia la omnipresencia de la Inteligencia Artificial en la vida de niños, niñas y adolescentes.

El 10 de febrero de 2026 la comunidad educativa global conmemorará una nueva edición del Día Internacional de Internet Seguro, una iniciativa impulsada por el Instituto Nacional de Ciberseguridad (INCIBE) y la Unión Europea. Bajo el lema "Seguridad Digital para Educar en tiempos de IA", este año el foco se desplaza hacia la omnipresencia de la Inteligencia Artificial en la vida de niños, niñas y adolescentes.

DÍA DEL INTERNET SEGURO: SEGURIDAD DIGITAL PARA EDUCAR EN TIEMPOS DE IA

INTRODUCCIÓN

El 10 de febrero de 2026, la comunidad educativa global conmemorará una nueva edición del Día Internacional de Internet Seguro, una iniciativa impulsada por el Instituto Nacional de Ciberseguridad ([INCIBE](#)) y la Unión Europea. Bajo el lema "Seguridad Digital para Educar en tiempos de IA", este año el foco se desplaza hacia la omnipresencia de la Inteligencia Artificial en la vida de niños, niñas y adolescentes.

Esta jornada, celebrada simultáneamente en más de cien naciones, tiene como objetivo central sensibilizar a la sociedad sobre la urgencia de construir un entorno digital más seguro. La Inteligencia Artificial (IA) ha dejado de ser una promesa futurista para convertirse en un componente cotidiano en la vida de niños, niñas y adolescentes. Por tanto, resulta imperativo brindar soporte a las instituciones educativas para que capitalicen las ventajas de la IA, minimizando al mismo tiempo los riesgos y fomentando un uso ético y saludable, en consonancia con las estrategias vigentes en Europa y a nivel nacional.



LA EDUCACIÓN BAJO UN ENFOQUE DE SEGURIDAD

La integración de la IA en las aulas ofrece un potencial inmenso, tanto para la gestión escolar como para los procesos de aprendizaje, eliminando barreras tradicionales hacia un futuro más personalizado. Esto libera tiempo valioso para que los docentes

se dediquen a lo verdaderamente crucial, desde la automatización administrativa hasta el acompañamiento pedagógico personalizado del aprendizaje. Sin embargo, esta innovación conlleva una gran responsabilidad: equilibrar las oportunidades pedagógicas con la protección tanto de la privacidad y la seguridad de los datos como de la protección del desarrollo cognitivo de los estudiantes.

Las herramientas actuales permiten la adaptación de contenidos curriculares a las necesidades individuales del alumno. No obstante, esta mayor inmersión digital implica que los estudiantes pasan más tiempo conectados, aumentando su exposición a peligros del mundo digital como el ciberacoso, contenidos inadecuados y distracciones ladronas de la atención que, según estudios regionales, impactan el rendimiento académico.

RETOS ESPECÍFICOS EN LATINOAMÉRICA

Nuestra región enfrenta una dualidad compleja: la necesidad de acelerar la digitalización y la obligación de asegurar entornos digitales y físicos protegidos. Aunque es positivo que más del 50% de los docentes latinoamericanos ya integren herramientas digitales, la formación continua es indispensable para que puedan guiar a sus estudiantes en temas cruciales de seguridad digital. La innovación educativa trae consigo la responsabilidad ineludible de proteger la privacidad y los datos sensibles frente a las nuevas vulnerabilidades que introduce la IA.

AMENAZAS EN EL ENTORNO EDUCATIVO DIGITAL

A medida que aumenta el uso de plataformas educativas, también lo hace la exposición a diversos peligros digitales. La integración profunda de la IA hace urgente la defensa contra riesgos digitales que no son exageraciones, sino realidades tangibles. Las principales amenazas incluyen:

- **Vulnerabilidad de Datos Personales:** La IA procesa información masiva, desde datos biométricos hasta académicos. Sin blindaje adecuado, esto puede derivar en robos de información por ciberdelincuentes, con consecuencias legales y reputacionales para las Instituciones Educativas.

- **Ataques de Malware y Ransomware:** Las plataformas educativas son objetivos atractivos. Los atacantes pueden secuestrar sistemas escolares exigiendo rescates o interrumpir las clases mediante software malicioso.
- **Ingeniería Social Sofisticada:** Los ataques de *phishing* ahora pueden simular interacciones mediante IA para engañar a usuarios y robar credenciales, haciendo la manipulación mucho más difícil de detectar.
- **Exposición a Contenido Nocivo:** Los algoritmos generativos pueden, inadvertidamente, exponer a los menores a desinformación, discursos de odio o material ilícito, afectando su bienestar.
- **El uso indebido de la IA:** Por último, y no menos importante, el uso indebido de la IA conlleva en muchos casos obstaculizar el aprendizaje, tergiversar el trabajo de los alumnos o introducir contenidos sesgados o no verificados en el aula.

Los marcos normativos, estándares y directrices globales para el uso de la IA en educación, con énfasis en las recomendaciones de la UNESCO y otras organizaciones internacionales, establecen principios fundamentales como la transparencia, la privacidad, la equidad y la inclusión, junto con recomendaciones para una adopción ética y efectiva de la IA en instituciones educativas. El enfoque SAFE (Seguras, Apropriadadas, Funcionalmente específicas y Económicamente viables) propone el desarrollo de soluciones tecnológicas para el éxito global de la IA en la educación:



EJEMPLOS DE MAL USO DE LA IA EN EL AULA

El mal uso de la tecnología no es un problema del futuro, ya está ocurriendo en las aulas y se manifiesta de diversas formas: cuando los estudiantes presentan tareas generadas por IA como propias o cuando los docentes dependen excesivamente de ella para planificar ambientes de aprendizaje sin hacer críticamente sus aportes. Esto puede llevar a un aprendizaje superficial, a la pérdida de atención y a la obstaculización del desarrollo del pensamiento crítico.

A continuación, desglosamos situaciones reales observadas en entornos escolares y analizamos sus implicaciones:

1. Tareas escritas por IA: Esta es la forma más común de uso indebido. Por ejemplo, el estudiante ya no solo "copia y pega" de una enciclopedia o de una página de internet localizada a través de un buscador, sino que utiliza un *prompt* en ChatGPT para generar un Ensayo sobre un tema que no ha estudiado ni domina, retocándolo levemente para intentar evadir la detección y entregándolo como propio.

Desde la perspectiva de la psicología cognitiva (Flower & Hayes), la escritura no es solo un producto final, sino un proceso recursivo de planificación, traducción y revisión que estructura el pensamiento. Al delegar esto a la IA, el estudiante se salta la Zona de Desarrollo Próximo (Vygotsky); es decir, elimina el "esfuerzo productivo" necesario para pasar de lo que sabe a lo que está aprendiendo. Sin ese esfuerzo cognitivo, no

hay internalización del conocimiento.

2. La "Docencia Automatizada": Dependencia excesiva en la planificación

Profesores saturados de trabajo administrativo recurren a la IA para elaborar planes de clase o crear rúbricas, sin una revisión crítica. Esto genera clases genéricas, descontextualizadas y, a veces, con errores factuales, limitándose a la transmisión de datos fríos.

El modelo TPACK (Mishra & Koehler) establece que la tecnología debe integrarse con el conocimiento pedagógico y el disciplinar. Cuando el docente confía ciegamente en la IA, rompe este equilibrio, cayendo en un **Tecnocentrismo** (Papert) donde la herramienta dicta el contenido en lugar de las necesidades del alumno. Se pierde la "contextualización", elemento clave para el aprendizaje significativo.

3. El "Ilusionismo Académico": Eludir las tareas de aprendizaje

Los estudiantes usan IA para resumir lecturas obligatorias, resolver ecuaciones paso a paso sin comprender la lógica o parafrasear textos. Obtienen altas calificaciones en tareas formativas, pero fracasan estrepitosamente en evaluaciones presenciales o sumativas.

Según Marton y Säljö, los estudiantes pueden adoptar un "enfoque superficial" (cumplir con la tarea con el mínimo esfuerzo) o un "enfoque profundo" (entender el significado). La IA, mal utilizada, actúa como un catalizador del aprendizaje superficial, bloqueando el desarrollo de la Metacognición (Flavell). El estudiante pierde la capacidad de autoevaluar si realmente ha entendido un concepto o si solo tiene la "ilusión de competencia" proporcionada por la herramienta.

4. La "Caja Negra" de los Datos: Violación de la privacidad

En un intento por agilizar procesos, docentes o alumnos suben listas de calificaciones, reportes de conducta o datos sensibles a herramientas de IA públicas (gratuitas), sin saber que esos modelos se entrenan con dicha información.

Esto contraviene los principios de la Ciudadanía Digital (Ribble), específicamente en el eje de "Seguridad y Privacidad". Desde el punto de vista legal, vulnera normativas de

protección de datos. Teóricamente, expone a los menores a lo que Zuboff llama **Capitalismo de la Vigilancia**, donde sus datos educativos se convierten en mercancía conductual para terceros sin su consentimiento informado.

5. La "Evaluación Comprometida": IA en exámenes remotos

En entornos virtuales o híbridos, los estudiantes usan la IA como un consultor en tiempo real para responder exámenes. Sin un diseño de evaluación robusto, las calificaciones reflejan la capacidad de la IA, no del alumno.

En psicometría y pedagogía, la "validez de constructo" es fundamental. Si un examen pretende medir "razonamiento histórico" pero el estudiante usa IA, la prueba pierde su validez porque está midiendo "habilidad de uso de herramientas". Se produce una distorsión en la **Evaluación Auténtica**, impidiendo que el docente identifique las brechas de aprendizaje reales del estudiante que requieren refuerzo.

6. La "Ciencia Ficticia": Generación de datos falsos

Ante la frustración de proyectos de investigación que no arrojan resultados claros, algunos estudiantes piden a la IA que genere tablas de datos "realistas" que confirmen sus hipótesis, fabricando evidencia científica.

Esto ataca la base del **Método Científico** y la falsabilidad. Pedagógicamente, obstaculiza el desarrollo del pensamiento crítico y mina la ética profesional. Al evitar el "fracaso" de una hipótesis (que es parte natural de la ciencia), el estudiante no aprende a lidiar con la incertidumbre ni a analizar la realidad, fomentando el sesgo de confirmación automatizado.

ESTRATEGIAS PARA UNA INTEGRACIÓN ÉTICA Y SEGURA DE LA IA EN EL AULA

Prevenir el uso indebido de la Inteligencia Artificial no requiere reinventar la pedagogía, sino adaptar nuestras mejores prácticas de gestión del aula al siglo XXI. Una propuesta se basa en tres pilares: establecer expectativas claras, modelar la integridad académica y construir confianza.

Del mismo modo que la educación integró la calculadora o los motores de búsqueda, el objetivo actual no es la prohibición que a menudo resulta contraproducente, sino la

alfabetización. Debemos enseñar a los estudiantes a navegar esta tecnología con prudencia, ética y sentido crítico.

A continuación, presentamos una hoja de ruta para los docentes e instituciones:

A) Estrategias pedagógicas de prevención y gestión

1. Co-creación de un "Marco Normativo del Aula"

Si el estudiante desconoce los límites, trazará los suyos propios. La ambigüedad es el terreno fértil para el plagio involuntario.

- Acción: Antes de iniciar cualquier unidad didáctica, defina explícitamente el rol de la IA. ¿Está permitido usarla para lluvias de ideas (*brainstorming*)? ¿Se acepta para corregir gramática, pero no para redactar argumentos?
- Estrategia: Redacte una política de uso aceptable y revísela periódicamente. Involucre a los estudiantes en la redacción de estas normas; cuando ellos participan en la creación de las "reglas del juego", su compromiso con el cumplimiento aumenta significativamente.

2. Alfabetización Algorítmica: Desmitificar la "Caja Negra"

El mal uso a menudo nace de la ignorancia sobre cómo funciona la herramienta. Muchos alumnos creen erróneamente que la IA es una "enciclopedia que habla", cuando en realidad es un modelo probabilístico que predice palabras.

- Acción: Dedique sesiones a explicar que la IA no "sabe" cosas; calcula probabilidades a través de los algoritmos
- Conceptos clave: Integre lecciones sobre "Alucinaciones" (cuando la IA inventa datos convincentes) y Sesgos Algorítmicos (prejuicios heredados de sus datos de entrenamiento). Esto encaja transversalmente en asignaturas de Lengua, Ciencias Sociales o Tecnología.

3. Cultura de la atribución y transparencia

Debemos cambiar la narrativa: usar IA no es un tabú si se declara honestamente. Fomentar la transparencia elimina la necesidad de ocultar el uso de herramientas de apoyo.

- Acción: Normalice la citación de la IA. Establezca protocolos sencillos, como incluir una nota al pie: *"Se utilizó ChatGPT para mejorar la cohesión de este párrafo"* o *"Argumentos iniciales explorados con ayuda de Gemini"*.
- Estrategia: Pida a los alumnos que entreguen el "antes y después" o que reflexionen sobre qué modificaron de la respuesta de la IA. Esto transforma la herramienta en un asistente, no en un sustituto del pensamiento.

4. El Docente como "Humano en el Bucle"

La IA puede ser un excelente copiloto para el docente, pero nunca el piloto automático.

- Acción: Utilice la IA para generar borradores de rúbricas, resumir textos densos o crear bancos de preguntas, crear recursos educativos, pero aplique siempre su criterio profesional para la edición final.
- Advertencia: No delegue la corrección ni el feedback emocional a la máquina. Al modelar un uso responsable y supervisado, usted enseña con el ejemplo.

5. Reingeniería de la Evaluación (Evaluación a prueba de IA)

Si una IA puede resolver una tarea en segundos, quizás la tarea deba evolucionar.

- Acción: Migre hacia formatos que valoren el proceso sobre el producto final.
- Estrategias:

Defensas orales: Donde el estudiante explique su razonamiento.

- Escritura en el aula: Retornar al papel y lápiz para fases creativas.
- Evaluaciones adaptativas: Cuestionarios que cambian según el desempeño del alumno.
- Metacognición: Preguntar "*¿Por qué elegiste esta fuente?*" es algo que la IA difícilmente puede responder con autenticidad personal.

B) Decálogo de seguridad digital para el estudiante

Más allá de lo académico, es vital proteger la identidad digital de los menores. Estas son las directrices de seguridad esenciales que todo docente puede transmitir a sus estudiantes:

1. Blindaje de la Identidad (Privacidad ante todo)

Instruya a los estudiantes para que **nunca** compartan Información de Identificación Personal (PII) con chatbots. Esto incluye nombres completos, direcciones, teléfonos, datos bancarios o detalles sobre su familia. Una vez que los datos entran en el modelo, se pierde el control sobre ellos.

2. Gestión activa de la privacidad

Enseñe a navegar por los menús de "Configuración" de las herramientas de IA. Muestre cómo desactivar el historial de chat o cómo solicitar que sus datos no se utilicen para entrenar versiones futuras del modelo.

3. Escepticismo saludable y verificación

Inculque el hábito de la verificación cruzada (*Fact-checking*). Antes de aceptar una respuesta, el estudiante debe triangular la información con fuentes primarias o libros de texto. La IA debe ser el punto de partida de la investigación, nunca la conclusión incuestionable.

4. Integridad Audiovisual (Alerta ante Deepfakes)

Lo que vemos y oímos ya no es garantía de realidad. Eduque sobre la existencia de manipulaciones de video y voz. Fomente un doble compromiso ético: Nunca usar IA para crear contenido falso que humille o suplante a compañeros o docentes. Analizar críticamente el contenido multimedia viral.

5. Autonomía Cognitiva (Evitar la dependencia)

Advierta sobre el riesgo de la "pereza cognitiva". Si delegan todas las decisiones o redacciones a la IA, pierden la oportunidad de desarrollar sus propias competencias. Explique que presentar trabajo generado por IA como propio constituye **plagio** y viola la integridad académica.

6. Actualización Continua

La tecnología evoluciona más rápido que los libros de texto. Anime a los estudiantes a mantenerse informados sobre las capacidades y riesgos de las nuevas versiones de IA. Un usuario informado es un usuario empoderado que toma decisiones conscientes, no impulsivas.

C) Gestión Institucional: Construyendo un ecosistema escolar seguro

Para que las estrategias en el aula sean efectivas, deben estar respaldadas por una estructura institucional sólida. La prevención del mal uso de la IA no es solo tarea del docente, sino un desafío de gobernanza escolar. A continuación, se presentan las líneas de acción que los equipos directivos y administrativos pueden adaptar e implementar en el entorno educativo:

1. Marco normativo y políticas de uso aceptable (PUA)

Más que simples prohibiciones, las instituciones deben desarrollar un "marco normativo Digital escolar", que permita definir protocolos y establecer directrices explícitas que regulen no solo qué dispositivos y aplicaciones están permitidos, sino *cómo* y *cuándo* pueden usarse.

Las Políticas de Uso Aceptable deben desglosar las consecuencias del plagio asistido por IA, el ciberacoso y la vulneración de seguridad, asegurando que toda la comunidad entienda la distinción entre uso pedagógico y abuso tecnológico.

2. Acompañamiento docente y supervisión pedagógica

La tecnología no puede operar en "piloto automático". La presencia humana sigue siendo el factor de control más importante. Un Monitoreo Activo en el aula evoluciona de "vigilar pantallas" a "acompañar procesos". Los docentes deben ser capacitados para identificar patrones de uso de IA y guiar a los estudiantes en tiempo real.

Además, las instituciones educativas deben garantizar que los recursos tecnológicos cuenten con filtros de contenido y medidas de seguridad que faciliten esta supervisión sin invadir injustificadamente la privacidad.

3. Alfabetización digital crítica como eje transversal

La mejor defensa contra la desinformación y el mal uso es una mente crítica. La enseñanza del pensamiento crítico no debe ser un taller aislado, sino una competencia transversal. Los estudiantes deben aprender a auditar la veracidad de la información en línea, comprender los sesgos algorítmicos y evaluar los riesgos éticos de sus huellas digitales.

4. Alianza Familia-Escuela y control parental

La educación digital es una responsabilidad compartida que trasciende los muros de la escuela. Orientar y empoderar a las Familias en la configuración de controles parentales y límites de tiempo de pantallas y el uso de dispositivos tecnológicos en el hogar. Ofrecer talleres sobre las nuevas tendencias de IA ayuda a reducir la brecha generacional, permitiendo que los tutores supervisen y comprendan el entorno digital en el que navegan sus hijos.

5. Blindaje de la privacidad y seguridad de datos

En la era del *Big Data*, la escuela es custodia de información sensible de menores. Hay que asegurar que todas las plataformas contratadas cumplan con las leyes de protección de datos locales e internacionales. Los datos de los estudiantes (biométricos, académicos y conductuales) deben ser intransferibles y utilizados estrictamente con fines pedagógicos, nunca comerciales.

6. Monitoreo de impacto y mejora continua

La tecnología cambia constantemente; por ello, las estrategias escolares no pueden permanecer estáticas. Es fundamental implementar ciclos de revisión basados en evidencia para medir el impacto real en el aprendizaje y cuestionarse: ¿la IA está mejorando los resultados o fomentando la dependencia? El análisis de estos datos permitirá ajustar las estrategias pedagógicas y de seguridad con la agilidad necesaria.

7. Democratización y equidad tecnológica

El acceso a la IA avanzada no puede convertirse en un nuevo privilegio que profundice desigualdades. La institución debe garantizar que todos los estudiantes, independientemente de su situación socioeconómica, tengan acceso equitativo a los dispositivos y la conectividad necesarios. Lo que implica buscar soluciones activas para los estudiantes desconectados.

8. Gobernanza participativa

Se deben crear comités de tecnología que incluyan a padres, estudiantes y docentes en la toma de decisiones. Cuando la comunidad participa en la definición de los "contratos sociales" digitales, se promueve una cultura de autorregulación y colaboración efectiva mucho más potente que la simple vigilancia.

La inteligencia artificial no llegó para reemplazar la creatividad, sino para desafiarla y potenciarla. Como educadores, tenemos la responsabilidad de abrir el diálogo, invitando a los estudiantes a ver estas herramientas como trampolines para el aprendizaje y no como atajos. Al fomentar un pensamiento crítico riguroso, les enseñamos a cuestionar la información, identificar sesgos y valorar su propia voz por encima del algoritmo.

La transparencia es la base de la confianza, si utilizamos como docentes la IA para planificar nuestras clases, debemos comunicarlo abiertamente. Este simple acto de honestidad modela la integridad académica que esperamos de los estudiantes.

Por último, ante la duda, defina las reglas. No debemos olvidar que la tecnología, por avanzada que sea, carece de empatía y comprensión emocional. La conexión humana sigue siendo el corazón del aula. Si su institución aún no cuenta con políticas claras, no espere; establezca normas éticas en su clase y lideré el camino hacia una cultura

digital responsable, donde la IA sea una herramienta al servicio del potencial humano.

Material de consulta:

- **La opinión de un educador: Cómo prevenir el mal uso de la IA en la educación**
- Adam De Gree <https://www.taotesting.com/es/blog/misuse-of-ai-in-education/> 23 de julio de 2025
- **Más del 50% de los docentes en Latinoamérica ya usan herramientas digitales en sus clases: un paso hacia el futuro educativo - Edutechnia -** <https://www.linkedin.com/pulse/m%C3%A1s-del-50-de-los-docentes-en-latinoam%C3%A9rica-ya-usan-herramientas-p09ce/>
- Día de Internet Segura 2026 <https://www.incibe.es/eventos/sid>
- Internet seguro, recomendaciones para educadores, padres y estudiantes <https://eduteka.icesi.edu.co/articulos/InternetSeguro>
- Plan de estudio para promover ciudadanos digitales responsables <https://eduteka.icesi.edu.co/articulos/google-se-genial-en-internet>

CRÉDITOS:

Artículo elaborado por Jorge Burbano y Juan Carlos López-García, Centro Eduteka.

Publicación de este documento en EDUTEKA: Febrero 9 de 2026.

Última actualización de este documento: Febrero 9 de 2026.