

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

[DOI 10.35381/cm.v12i22.2084](https://doi.org/10.35381/cm.v12i22.2084)

Gestión de riesgos y seguridad como segunda dimensión ética de la inteligencia artificial en educación

Risk management and security as the second ethical dimension of artificial intelligence in education

Jennifer Andreina Duque-Rodríguez
phd.jennifer11@gmail.com

Red de Investigación Koinonía, Maracaibo, Zulia
Venezuela

<http://orcid.org/0000-0002-2349-2525>

Lenys Senovia Piña-Ferrer
lenyspina@iieakoinonia.org

Instituto de Investigación y Estudios Avanzados Koinonía, Santa Ana de Coro, Falcón
Venezuela

<https://orcid.org/0000-0002-9493-7499>

Josía Jeseff Isea-Argüelles
ui.josiaia82@uniandes.edu.ec

Universidad Regional Autónoma de los Andes, Ibarra, Imbabura
Ecuador

<https://orcid.org/0000-0001-8921-6446>

Recepción: 25 de agosto 2025
Revisado: 26 de noviembre 2025
Aprobación: 13 de diciembre 2025
Publicado: 01 de enero 2026

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

RESUMEN

El presente estudio tuvo como propósito analizar la gestión de riesgos y el cumplimiento de protocolos de seguridad como segunda dimensión ética de la inteligencia artificial en educación. Metodológicamente, se sustentó en las orientaciones de la investigación documental y el método analítico. Como técnica, se acudió a la revisión sistemática y al análisis de contenido y, como instrumento, se emplearon las fichas de registro y las matrices de análisis. También se procesó la declaración PRISMA para la selección de los estudios. Como resultado, se destacó la importancia de orientar cualquier acción desde una finalidad formativa y constructiva, protegiendo la autonomía humana desde orientaciones éticas para la incorporación de la IA, sugiriendo la evaluación constante para atender los riesgos emergentes. Como conclusión, los protocolos de seguridad y la gestión de datos en entornos educativos destacaron como elementos clave para manejar los datos en función de lograr buenas prácticas de desarrollo seguro.

Descriptores: Inteligencia artificial; gestión de riesgos; protocolos de seguridad; inteligencia artificial en educación. (Tesauro UNESCO).

ABSTRACT

The purpose of this study was to analyze risk management and compliance with security protocols as a second ethical dimension of artificial intelligence in education. Methodologically, it was based on documentary research and analytical methods. Systematic review and content analysis were used as techniques, and record sheets and analysis matrices were used as instruments. The PRISMA statement was also processed for the selection of studies. As a result, the importance of guiding any action from a formative and constructive purpose was highlighted, protecting human autonomy from ethical guidelines for the incorporation of AI, suggesting constant evaluation to address emerging risks. In conclusion, security protocols and data management in educational environments stood out as key elements for handling data in order to achieve good practices for secure development.

Descriptors: Artificial intelligence; risk management; security protocols; artificial intelligence in education. (UNESCO Thesaurus).

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

INTRODUCCIÓN

Actualmente, es importante resaltar la preocupación sobre la gestión de riesgos asociados a la seguridad y el bienestar del ambiente de aprendizaje cuando se emplea la IA desde la ética (Zhu et al., 2025). La inteligencia de los algoritmos de aprendizaje automático se logra entrenándolos con altas cantidades de datos. En el caso de la educación implica el uso de información disponible en la escuela de los estudiantes y sus familias. En algunos casos, el uso de las redes sociales u otra información, mediante la grabación de imágenes, video y audio, a fin de crear aplicaciones de personalización de respuestas (Duque et al., 2025a).

Otro riesgo a considerar está representado por los protocolos de seguridad y la gestión de datos por parte de las empresas que desarrollan sistemas y aplicaciones educativas. Este es un tema de interrogantes y debate, por cuanto requiere enfatizar en el uso ético, de carácter restrictivo y limitado de fines académicos de la información personal de los estudiantes que, en oportunidades son menores de edad. Se debe evitar que la información sea utilizada para objetivos distintos para los que están autorizados, pudiendo convertirse en víctimas de manipulación comercial o de otro tipo (Leong & Zhang, 2025).

En el ámbito educativo, es necesario que cada institución establezca sus protocolos para gestionar los riesgos, a través de acciones específicas que permitan aprovechar los beneficios de la IA en conjunción con la misión y la visión institucional. Se deben mostrar atención a los requisitos legales o regulatorios para enriquecer los procesos educativos en función de propiciar una educación integral con sentido humanista (Zhu et al., 2025). A partir de lo anterior, es necesario proteger los datos de los docentes, estudiantes y familiares por medio de las herramientas que ofrece la IA, en pro de garantizar el cuidado de la integridad física y mental de estos por medio de un proceso ético. De este modo, aprovechando el apoyo de la IA como asistente de los distintos acontecimientos que se vivencian en el contexto educativo, es fundamental entenderla como un mecanismo

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

robusto y confiable capaz de facilitar la preservación de la autonomía y dignidad de los estudiantes, quienes fungen como protagonistas del acontecer pedagógico.

Tomando en consideración los aspectos antes descritos, emergió la presente investigación que tuvo como propósito analizar la gestión de riesgos y el cumplimiento de protocolos de seguridad como segunda dimensión ética de la inteligencia artificial en educación por medio de la revisión sistemática documental.

METODOLOGÍA

El presente estudio se caracterizó por desarrollarse siguiendo las orientaciones de la investigación documental. El propósito principal fue dirigir la investigación desde dos aspectos: relacionando datos ya existentes que proceden de distintas fuentes y proporcionando una visión panorámica y sistemática de una determinada cuestión elaborada en múltiples fuentes dispersas. Se consideran estudios previos con carácter científico para identificar los aspectos claves que permitan el análisis de las dimensiones éticas de la inteligencia artificial en educación (Isea et al., 2024).

Para ello, se empleó el método analítico, cuyo enfoque permitió distinguir las partes dentro de un todo. Se interpretaron cada elemento por separado en secuencia para realizar un análisis de la gestión de riesgos asociados a la seguridad y bienestar del ambiente de aprendizaje con IA. Se utilizó la información de fuentes bibliográficas, a través de datos relevantes contenidos en artículos científicos, tesis y el material narrativo y audiovisual relacionado (Zhu et al., 2025).

La declaración PRISMA se tomó como base para la selección de los artículos. De este proceso, se seleccionaron 12 artículos correspondientes a las bases de datos Scielo, Scopus y Web of Science.

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

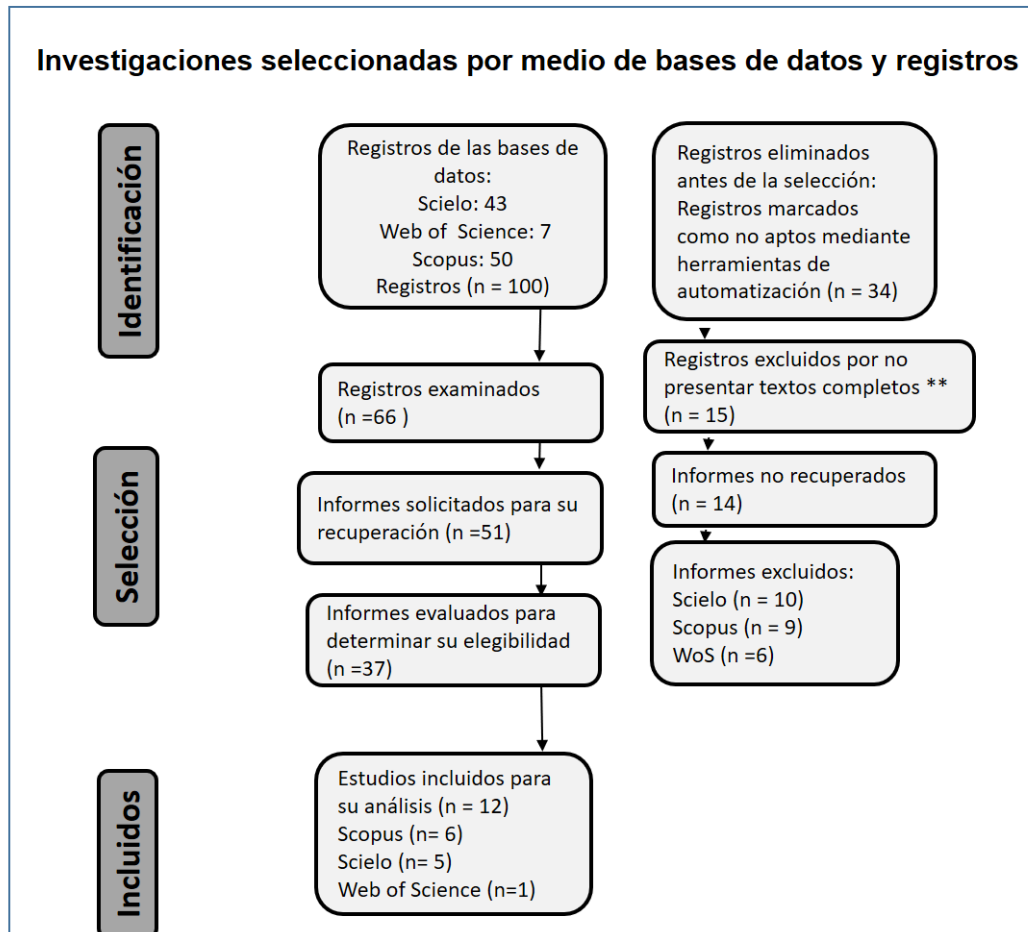


Figura 1. Pasos de la declaración PRISMA para la selección de los artículos.
Elaboración: Los autores.

Tal como se puede evidenciar en la figura 1, al inicio, se identificaron 100 artículos en total; es decir, 43 de Scielo, 7 de Web of Science y 50 de Scopus. De tales artículos, se examinaron 66; luego 51 fueron solicitados para su recuperación, 37 fueron evaluados para determinar su elegibilidad, siendo finalmente, 12 incluidos para sus análisis; específicamente, 6 de Scopus, 5 de Scielo y 1 de WoS.

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

RESULTADOS

El resultado del estudio está conformado por el análisis de los elementos planteados como segunda dimensión de la inteligencia artificial: Gestión de riesgos (GRS) y cumplimiento de protocolos de seguridad. Se tomaron en consideración los planteamientos de Duque et al. (2025a; 2025b); Santana et al. (2024); Isea et al. (2024), Leong et al. (2025), entre otros.



Figura 2. Segunda dimensión ética de la inteligencia artificial en la educación.

Elaboración: Los autores.

Gestión de riesgos asociados a la seguridad y bienestar del ambiente de aprendizaje con IA

Según la figura 2, en el ámbito educativo, al momento de planificar o programar cualquier actividad que tiene una finalidad formativa y constructiva, se tomaron en consideración los materiales y recursos tanto físicos como humanos necesarios para el desarrollo armonioso y el alcance de los propósitos establecidos. En ese sentido, es importante y

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

necesario que, al momento de incorporar el uso de herramientas tecnológicas y de inteligencia artificial, se tengan en cuenta los aspectos esenciales a nivel técnico que puedan afectar la seguridad y el bienestar del entorno de aprendizaje (Duque et al., 2025b; Santana et al., 2024).

Con ello, es importante reforzar las estrategias que puedan ser consideradas para proteger la autonomía humana, en función de resguardar el ingenio y mantener la tecnología como una herramienta de apoyo que guíe la atención a lo importante. De esta forma se protege la libertad de expresión y creatividad, siendo requerido una constante supervisión y revisión crítica, fomentando espacios para la higiene digital al propiciar actividades de aprendizaje que favorezcan la creación y la socialización de ideas sin tecnología, a fin de fortalecer el pensamiento crítico e independiente, manteniendo la integridad al declarar el uso de la IA.

De igual modo, se resalta el crecimiento del uso de las herramientas de IA por parte de los estudiantes al momento de realizar actividades variadas, en oportunidades, por curiosidad personal y otras veces por recomendación de sus instructores. Es necesario que, al momento en el cual los docentes realizan la sugerencia del uso de la herramienta tecnológica para tareas e investigaciones, se encuentren acompañadas de orientaciones claras y recomendaciones éticas para su uso sin comprometer la seguridad y el bienestar. Las recomendaciones deben estar establecidas en las normativas institucionales o manuales de convivencia para asegurar que la información sea recibida, atendida y entendida por todos los actores educativos (Duque et al., 2025b; Isea et al., 2024).

En ese sentido, se manifiesta que los estudiantes demuestran satisfacción por el uso de la IA porque pueden encontrar respuestas rápidas, automatizar procesos o personalizar las experiencias de aprendizaje. Además de esos usos en el contexto académico, las herramientas impulsadas por IA desempeñan un papel igualmente importante en el

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

entretenimiento, ya que los estudiantes utilizan estos sistemas para participar en las redes sociales, juegos u otras formas de interacción digital durante su tiempo libre.

De esa manera, la incorporación de la IA en las redes sociales a los entornos de aprendizaje implica estar atento a las posibles amenazas emergentes desde múltiples aspectos. Una de ellas se enfoca en las vulnerabilidades que se pueden presentar ante alguna falla en el resguardo de los datos que comprometa el sentido ético institucional con respecto al uso de las herramientas tecnológicas. Por otro lado, desde la perspectiva del estudiante, aunque no perciba los peligros de forma directa, la presencia de algoritmos en las redes sociales forma parte de un riesgo que puede perjudicar la seguridad digital y el entorno de aprendizaje en general (Leong y Zhang, 2025).

En este sentido, Torres et al. (2025) estiman tener presente que las aplicaciones basadas en IA siguen evolucionando. A su vez, es necesario evaluar constantemente tanto los aspectos positivos como los negativos de su uso, siendo esencial para crear estrategias informadas que promuevan el éxito académico y el bienestar integral de los estudiantes. Por ello, desde el primer momento en el cual se usan las herramientas de inteligencia artificial, se enfatice en los aspectos básicos que permitan gestionar los riesgos asociados a la seguridad. Se persigue evitar la discriminación, exclusión social e incremento de la brecha digital por escasas inversiones de ciberseguridad que faciliten los ataques a los entornos de aprendizaje digital debido a las vulnerabilidades. A ellos se agregan los riesgos de exposición y privacidad por memorización de datos personales, huellas digitales o información detallada que pueda ser empleada en patrones de reconocimiento (Aparicio et al., 2023; García et al., 2026).

La figura 3 resume la gestión de riesgos asociada a la seguridad y bienestar del ambiente de aprendizaje con IA. Se expone lo relacionado a la atención a los riesgos, la evaluación, la incorporación de la IA en las redes sociales, la finalidad formativa y constructiva, la protección de la autonomía humana y las recomendaciones éticas.

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles



Figura 3. Gestión de riesgos asociados a la seguridad y bienestar del ambiente de aprendizaje con IA.
Elaboración: Los autores.

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

Protocolos de seguridad y gestión de datos por quienes desarrollan sistemas de aplicaciones educativas

El tratamiento y resguardo de la información es un tema relevante en el desarrollo de sistemas, porque en la medida en la cual prospera la tecnología, se hace necesario el incremento de protocolos de seguridad para proteger a los usuarios procurando, a su vez, aminorar las vulnerabilidades de los datos. Al respecto, se enfatiza en la importancia de la privacidad y el control de los datos para evitar vulnerabilidades como derecho humano que debe ser respetado por todas las personas; por tanto, las organizaciones deben dirigir sus procedimientos con la intención de cuidar la confidencialidad, la integridad y la disponibilidad de la información (Duque et al., 2025b).

Al respecto, se argumenta que la compilación y uso de datos personales en plataformas digitales ameritan la actualización de las normativas de la protección de datos para que los usuarios puedan tener mayor control sobre su información (Mendoza et al., 2024). De allí que se considere la privacidad como un derecho humano que implica la vida privada, la protección de los datos personales y el control sobre la información personal.

Por ende, se persigue que el uso de tecnologías y de la IA en el ámbito educativo se encuentre acompañado por la necesidad de atender la seguridad como tema neurálgico para el bienestar de los actores educativos; es, en este caso, donde los protocolos adquieren protagonismo para prevenir y tener capacidad de respuesta ante situaciones de riesgo, al tener establecidos los procedimientos a seguir ante las posibles amenazas que se puedan presentar en el entorno educativo digital.

Por lo anterior, es importante generar ambientes de aprendizaje positivos en los que resulten evidentes los esfuerzos para mantenerlos seguros, reforzando la confianza de la comunidad en general al cumplir con las regulaciones establecidas e incluso contar con un esquema normativo interno de la institución que especifique los procedimientos en los cuales se tenga como prioridad la protección de datos personales de los estudiantes para avalar la seguridad y privacidad en línea y fuera de ella. En este sentido,

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

se persigue tener la capacidad de detectar el acoso escolar producido en esquemas digitales, prevenir contenido digital asociado al abuso de sustancias, promover la salud mental y bienestar de los actores educativos (Sánchez et al., 2025).

Para lograrlo, los desarrolladores de sistemas de aplicaciones educativas requieren la consideración para implementar protocolos de seguridad que se distingan por atender los elementos técnicos fundamentales como la protección de datos en tránsito y reposo, la autenticación y autorización para la gestión rigurosa de las contraseñas que permitan contrarrestar intentos de acceso no autorizados, seguridad en el desarrollo al tener en cuenta las normativas estándar para la gestión de riesgos, el cifrado de datos sensibles, el monitoreo constante acompañado de auditorías con respecto al acceso de la plataforma para detectar comportamientos inusuales (Mendoza et al., 2024; Batista-Barallobre, 2025).

Lo anterior son algunas de las consideraciones clave a las que deben añadirse las indicadas por las especificidades y conocimientos técnicos propios del área de programación, así como las señaladas por los respectivos reglamentos y marcos legales vigentes que atiendan la protección de los usuarios. De manera específica, la de los estudiantes quienes, como menores de edad, gozan de amparo en función del resguardo de sus derechos; lo cual, contribuye al fortalecimiento de los procesos educativos desarrollados.

En ese marco de ideas, es preciso indicar la importancia de la gestión de datos para la recolección, organización, almacenamiento y resguardo de la información con garantías de integridad, confidencialidad, disponibilidad y cumplimiento normativo para la gestión, protección, seguridad y privacidad de estos.

La figura 4 sintetiza los protocolos de seguridad y la gestión de datos por quienes desarrollan sistemas de aplicaciones educativas, resumiendo la intención de los protocolos de seguridad, los temas neurálgicos de atención, los elementos distintivos, la gestión de datos y las buenas prácticas de desarrollo seguro.

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

Consideraciones clave de los protocolos de seguridad y gestión de datos en entornos educativos

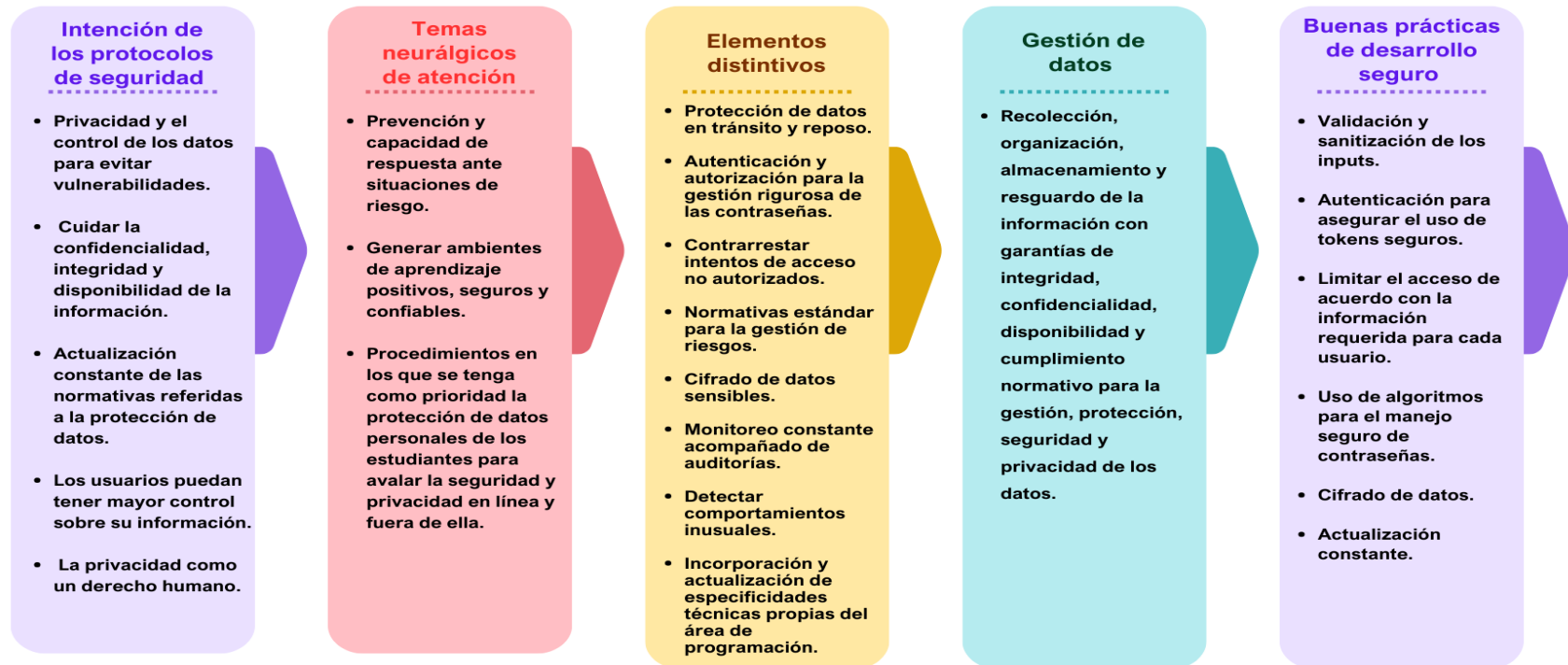


Figura 4. Protocolos de seguridad y gestión de datos por quienes desarrollan sistemas de aplicaciones educativas
Elaboración: Los autores.

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

Enfatizar en el uso ético e incluso restrictivo de información personal como parte de la gestión de riesgos en el uso de la IA

De acuerdo con Morales et al. (2024), la ética en la IA debe abordar aspectos tanto ético como morales, identificando los desafíos inherentes a la transparencia, sesgos, discriminación, privacidad y seguridad de los datos, rendición de cuentas, impacto social y económico; aunado a ello, se indica que todo ello se traduce en la necesidad de tener en cuenta que el uso ético y restrictivo de la información en la Inteligencia Artificial (IA) se fundamenta en principios que buscan proteger la autonomía humana y la privacidad, limitando cómo los algoritmos acceden y procesan datos.

En tal sentido, la Organización de Estados Americanos, en el año 2021, presenta una actualización sobre la Privacidad y la Protección de Datos Personales, que fueron aprobados por unanimidad el 9 de abril de 2021 por el Comité Jurídico Interamericano (CJI). La actualización fue organizada en trece (13) principios que buscan modernizar el marco normativo de las américas, adaptándolo a los retos de la economía digital:

1. **Finalidades legítimas y lealtad** resaltando que los datos personales deberían ser recopilados únicamente con fines legítimos y medios leales. Los datos deben tratarse de forma justa, legal y con información clara al titular.
2. **Transparencia y consentimiento:** El tratamiento de la información debe sustentarse en el consentimiento libre, inequívoco, previo e informado (salvo excepciones legales).
3. **Pertinencia y necesidad:** Solo deben solicitarse los datos necesarios y pertinentes para el fin propuesto.
4. **Tratamiento y conservación limitada:** Los datos personales deberían ser tratados y conservados de manera legítima no incompatible con el fin propuesto y su conservación no debe exceder el tiempo necesario para ello.
5. **Confidencialidad:** Se debe garantizar que personas no autorizadas no accedan a la información.

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

6. **Seguridad de los datos:** Implementación de medidas técnicas y organizativas para evitar la divulgación, pérdida, destrucción, acceso no autorizado o ilegítimo aun cuando ocurriera de manera accidental.
7. **Exactitud de los datos:** Los datos deben ser verídicos, exactos y mantenerse actualizados.
8. **Acceso, rectificación, cancelación, oposición y portabilidad:** Derecho de los titulares a solicitar acceso a sus datos, rectificación o eliminación; así como, de oponerse al tratamiento de la información. Todo ello, teniendo como regla general el carácter gratuito y cualquier restricción debe sustentarse en el marco jurídico aplicable.
9. **Datos personales sensibles:** Los responsables de los datos deberían adoptar y reforzar las medidas de privacidad y seguridad de acuerdo con la naturaleza de los datos acorde con la sensibilidad de los datos y la capacidad de hacer daño a sus titulares.
10. **Responsabilidad:** Los responsables o encargados del tratamiento de la información deben adoptar medidas apropiadas para el tratamiento de la información.
11. **Flujo transfronterizo de datos y responsabilidad:** Cooperación para la creación de mecanismos y procedimientos que aseguren el tratamiento de los datos al ser transmitidos a otra jurisdicción.
12. **Excepciones:** Cualquier excepción a alguno de los principios debe ser expresado claramente ante los entes u organismos competentes.
13. **Autoridades de protección de datos:** Comprende a los organismos independientes que garantizan el cumplimiento de los principios planteados.

Acciones para la gestión de riesgos para aprovechar los beneficios de la IA

Las acciones específicas para la gestión de riesgos en el uso de la Inteligencia Artificial (IA), se desarrollan con la intención de proteger de manera estratégica los procesos; para

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

ello, es esencial la valoración constante de riesgos, mantener los estándares de calidad, cumplir con responsabilidades para disminuir amenazas al aplicar procedimientos estandarizados y alineados con los debidos reglamentos, para garantizar la trazabilidad, la transparencia, información adecuada, supervisión humana y fiabilidad en el uso de las herramientas.

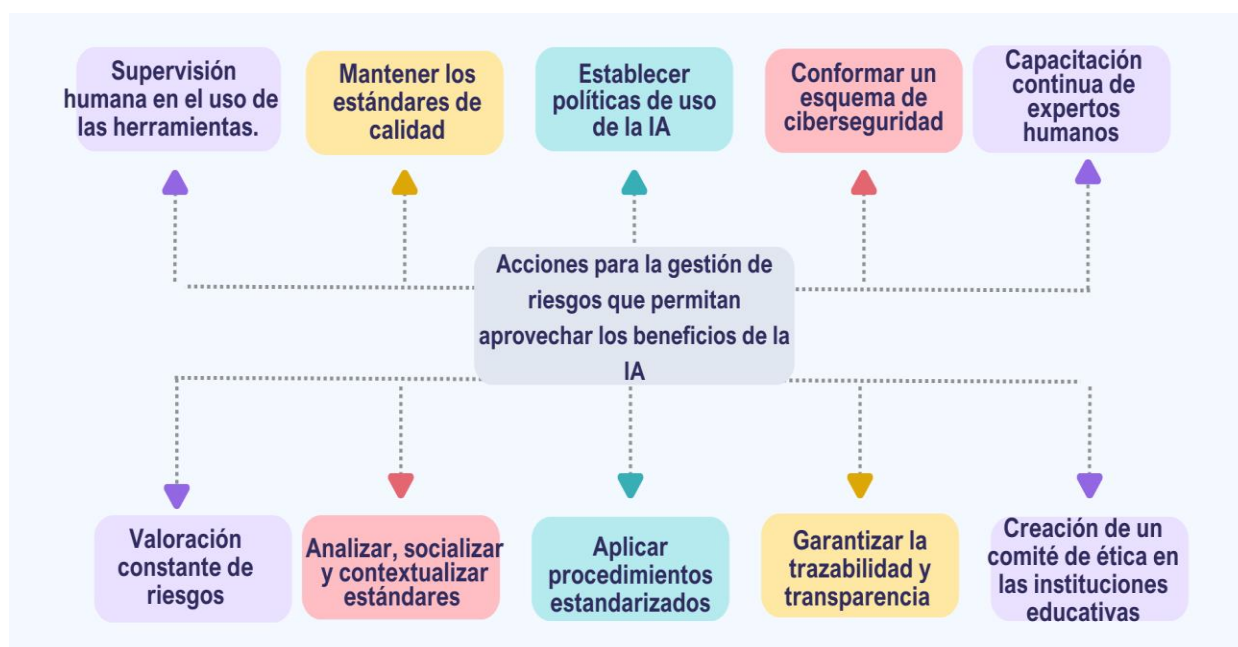


Figura 5. Acciones para la gestión de riesgos para aprovechar los beneficios de la IA.
Elaboración: Los autores.

En atención a los resultados presentados en la figura 5, se recomiendan impulsar acciones a la creación de un comité de ética en las instituciones educativas, generando espacios con la intención de analizar, socializar y contextualizar los estándares internacionales, nacionales y locales de acuerdo con los propósitos del centro escolar para de esa manera, establecer políticas de uso de la IA desde la seguridad jurídica y protección de los datos al desarrollar una gestión técnica acompañada de la combinación de métodos, procesos, herramientas y comportamientos que protegen los sistemas

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

informáticos en un esquema de ciberseguridad con constante validación de resultados y capacitación continua de expertos humanos para transformar una herramienta potente en una solución confiable y ética.

DISCUSIÓN

El resultado del presente estudio está conformado por el análisis de los elementos previamente planteados como segunda dimensión gestión de riesgos (GRS) y cumplimiento. En relación con la gestión de riesgos asociados a la seguridad y bienestar del ambiente de aprendizaje con IA, se destaca la importancia de orientar cualquier acción desde una finalidad formativa y constructiva, protegiendo la autonomía humana desde orientaciones éticas para la incorporación de la IA, sugiriendo la evaluación constante para atender los riesgos emergentes (Hurtado et al., 2024).

Aunado a ello, se presentan unas consideraciones clave de los protocolos de seguridad y gestión de datos en entornos educativos destacando la intención de abordar algunos temas neurálgicos de atención junto a elementos distintivos para gestionar los datos, en función de lograr buenas prácticas de desarrollo seguro. Alineado a ello, se enfatiza en el uso ético e incluso restrictivo de información personal como parte de la gestión de riesgos en el uso de la IA, desde la actualización sobre la Privacidad y la Protección de Datos Personales.

Cabe destacar que la consideración de la gestión de riesgos y los protocolos de seguridad contribuyen con el fomento de un marco de protección consolidado, el cual evita el ingreso a la privacidad de las personas y las resguarda, conservando así, la dignidad humana y la autonomía intelectual y física de docentes, estudiantes y sus familiares.

CONCLUSIONES

Los resultados del estudio condujeron a tener en cuenta las acciones para la gestión de riesgos que permitieran aprovechar los beneficios de la IA, entre las que destacan: la

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

supervisión humana en el uso de herramientas, mantener los estándares de calidad, establecer políticas de uso de la IA, conformar un esquema de ciberseguridad, capacitación continua de expertos humanos, creación de un comité de ética en las instituciones educativas, garantizar la trazabilidad y transparencia, aplicar procedimientos estandarizados, analizar, socializar y contextualizar estándares de acuerdo con la valoración constante de riesgos. Todo ello, con la intención de equilibrar la innovación educativa con la protección de la integridad física, emocional y digital de la comunidad escolar.

En síntesis, se enfatiza el uso ético e incluso restrictivo de información personal como parte de la gestión de riesgos en el uso de la IA, desde la actualización sobre la Privacidad y la Protección de Datos Personales, los cuales fueron aprobados por unanimidad el 9 de abril de 2021 por el Comité Jurídico Interamericano de la Organización de Estados Americanos.

Se plantean recomendaciones que conducen a la realización de otras investigaciones donde se profundice en el impacto de la gestión de riesgos y los protocolos de seguridad dentro de contextos educativos específicos. También se sugiere diseñar programas de capacitación docente y estudiantil para la detección de casos de abuso en la privacidad y así prepararse para enfrentar cualquier tipo de situación. Tales estudios pueden ser enfocados en diversos paradigmas ajustados a cada realidad educativa.

FINANCIAMIENTO

No monetario.

AGRADECIMIENTO

A todos los agentes sociales involucrados en el desarrollo de la investigación.

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

REFERENCIAS CONSULTADAS

- Aparicio, O., Ostos, O., y Von Feigenblatt, O. (2023). Competencia digital y desarrollo humano en la era de la Inteligencia Artificial. *Hallazgos*, 20(40), 217-235. <https://n9.cl/p7aeaa>
- Batista-Barallobre, A. R. (2025). Emergencia social en sistemas adaptativos complejos: una revisión sistemática desde la simulación basada en agentes. *Maestro y Sociedad*, 22(3), 2232-2245. <https://n9.cl/qz3317>
- Duque-Rodríguez, J. A., Piña-Ferrer, L. S., e Isea-Argüelles, J. J. (2025a). Tecnología, datos y seguridad como primera dimensión ética de la inteligencia artificial en educación. *EPISTEME KOINONIA*, 8(16), 186-208. <https://n9.cl/v5nh2>
- Duque-Rodríguez, J., Piña-Ferrer, L., e Isea-Argüelles, J. (2025b). Dimensiones éticas de la inteligencia artificial en educación. *CIENCIAMATRIA*, 11(20), 27-45. <https://doi.org/10.35381/cm.v11i20.1522>
- García Calle, D. F., Becilla Vera, M. L., Cordero Alvarado, N. I., Urgilés Carabajo, C. G., Solano Farias K. M., Ortiz Salas, D. A., et al. (2026). Modelos predictivos con inteligencia artificial: detección temprana de perfiles de diversidad comunicativa en educación médica superior. *Educación Médica Superior*, 40, 1-20. <https://n9.cl/t8yen>
- Hurtado, C., Villa, M., Caicedo, L., e Isea, J. (2024). A plithogenic statistical approach to digital security measures and emotional health in childhood and adolescence. *Journal of Fuzzy Extension and Applications*, 5(Special Issue), 25-39. <https://n9.cl/au5u0>
- Isea, J., Infante, M., Romero, A., y Comas, R. (2024). Human talent as a driving force in the management of ethics in the sustainable university. *Salud, Ciencia y Tecnología - Serie de Conferencias*, 3:672, 1-9. <https://n9.cl/jbjohe>
- Isea, J., Romero, A., y Molina, T. (2024). Ontology of the university teacher: a transformational leader in lifelong learning. *Health Leadership and Quality of Life*, 3:483, 1-8. <https://n9.cl/dhbk6>
- Isea, J., Duque, J., Piña, L., y Atencio, R. (2024). Analysis of artificial intelligence in the transformation of educational teaching and learning. *Revista Conrado*, 20(100), 179-185. <https://n9.cl/cyd00>

Jennifer Andreina Duque-Rodríguez; Lenys Senovia Piña-Ferrer; Josía Jeseff Isea-Argüelles

- Leong, W. Y., & Zhang, J. B. (2025). Ethical design of AI for education and learning systems. Diseño ético de la IA para sistemas educativos y de aprendizaje. *ASM Science Journal*, 20(1), 1-9. <https://n9.cl/kk8ped>
- Mendoza Vega, A. J., Guadamud Muñoz, J. D., Santana Castro, E. K., Chiriboga Palacios, I. A., y Vera Arias, M. J. (2024). Uso de las plataformas de inteligencia artificial en el contexto educativo. *Ciencia Latina Revista Científica Multidisciplinar*, 8(1), 10996-11009. <https://n9.cl/3eejhw>
- Morales, E. E., Santana, E. K., y Mendoza, A. J. (2024). Un crimen llamado educación digital: desafíos y dilemas en la era de la tecnología. A crime called digital education: challenges and dilemmas in the age of technology. *Estudios y Perspectivas. Revista Científica Y Académica*, 4(2), 1849-1862. <https://n9.cl/gk9qt>
- Sánchez, A., Zilberstein, J., Flores, I., y Peñalosa, M. (2025). Percepción de las implicaciones éticas en el uso de la Inteligencia Artificial. Perception of the ethical implications of using Artificial Intelligence. *Emerging trends in education (México, Villahermosa)*, 8(15), 89-104. <https://n9.cl/c5yab>
- Santana Castro, E. K., Morales Vásquez, E. E., González, C. D. J., Zambrano Rugel, M. H., Pérez Rodríguez, Y. V., y Mendoza Vega, A. J. (2024). Impacto de los Entornos Virtuales de Aprendizaje: Análisis de Revisión Documental. *Revista Veritas De Difusão Científica*, 5(2), 1623-1638. <https://n9.cl/sflqa>
- Torres, J., Fernández, O., y Ramírez, M. (2025). Prospectiva y futuro: políticas públicas y marco regulatorio para garantizar el uso ético y responsable de la IA en la educación superior. *Inter disciplina*, 13(37), 221-241. <https://n9.cl/0v8hzo>
- Zhu, H., Sun, Y., & Yang, J. (2025). Towards responsible artificial intelligence in education: a systematic review on identifying and mitigating ethical risks. *Humanities and Social Sciences Communications*, 12(1), 1-14. <https://n9.cl/f61lx>