Plataforma inteligente para la defensa proactiva de infraestructuras educativas sostenibles

Intelligent platform for the proactive defense of sustainable educational infrastructures

Recibido: 2025/10/07- Aceptado: 2025/11/07 - Publicado: 2025/11/18

Edison Javier Guaña Moya
Instituto Superior Universitario Japón, Quito, Ecuador
eguana@itsjapon.edu.ec
https://orcid.org/0000-0003-4296-0299

Resumen

El estudio examinó cómo las plataformas inteligentes ayudan a proteger las infraestructuras educativas sostenibles. Su objetivo es entender de qué manera la inteligencia artificial ética y adaptable mejora la seguridad digital y la sostenibilidad de las instituciones. La investigación se desarrolló mediante un enfoque cualitativo-documental basado en una revisión sistemática de literatura científica reciente, utilizando exclusivamente la base de datos Dimensions.ai. Se identificaron inicialmente 854 documentos y, tras aplicar filtros por periodo (2021–2025), acceso abierto y tipo de publicación, se obtuvo una muestra final de 96 artículos revisados por pares. El proceso siguió las directrices del protocolo PRISMA 2020, lo que permitió garantizar transparencia y trazabilidad en las etapas de identificación, cribado, elegibilidad e inclusión. Los resultados evidenciaron una concentración de producción académica en España y Argentina, y una creciente participación latinoamericana con predominio de estudios técnicos sobre los éticos o institucionales. Se identificaron tres tendencias principales: mejorar la ciberseguridad en la educación usando algoritmos de aprendizaje profundo, buscar una tecnología sostenible con modelos que consumen menos energía, y la integración progresiva de la gobernanza algorítmica y

la ética digital. Se llegó a la conclusión de que usar inteligencia artificial de manera responsable es clave para crear sistemas educativos sostenibles que logren un equilibrio entre innovación, igualdad y protección de datos. Se recomienda fomentar la cooperación interregional y desarrollar marcos normativos que aseguren la transparencia, la eficiencia y la sostenibilidad en la gestión tecnológica universitaria.

Palabras clave: Ciberseguridad, sostenibilidad tecnológica, inteligencia artificial, gobernanza digital, ética algorítmica.

Abstract

The study examined how smart platforms help protect sustainable educational infrastructures. Its objective is to understand how ethical and adaptable artificial intelligence enhances digital security and institutional sustainability. The research was conducted using a qualitative-documentary approach based on a systematic review of recent scientific literature, exclusively using the Dimensions.ai database. Initially, 854 documents were identified, and after applying filters for period (2021–2025), open access, and publication type, a final sample of 96 peer-reviewed articles was obtained. The process followed the PRISMA 2020 protocol guidelines, which ensured transparency and traceability in the identification, screening, eligibility, and inclusion stages. The results revealed a concentration of academic output in Spain and Argentina, and growing Latin American participation, with technical studies predominating over ethical or institutional ones. Three main trends were identified: improving cybersecurity in education using deep learning algorithms, pursuing sustainable technology with models that consume less energy, and the progressive integration of algorithmic governance and digital ethics. It was concluded that using artificial intelligence responsibly is key to creating sustainable educational systems that strike a balance between innovation, equality, and data protection. It is recommended to foster interregional cooperation and develop regulatory frameworks that ensure transparency, efficiency, and sustainability in university technology management.

Keywords: Cybersecurity, technological sustainability, artificial intelligence, digital governance, algorithmic ethics.

Introducción

La expansión de la digitalización en el ámbito educativo ha generado un ecosistema tecnológico cada vez más interconectado, donde la infraestructura digital se ha convertido en un componente esencial para garantizar la continuidad de los procesos de enseñanza, investigación y gestión institucional. No obstante, este avance ha venido acompañado de un aumento en las amenazas cibernéticas que afectan la integridad, disponibilidad y confidencialidad de la información académica. En este contexto, la protección de las redes educativas se ha vuelto un requisito estratégico para la sostenibilidad tecnológica y la confianza digital de las instituciones (Álvarez, 2022; Acosta, 2023). La literatura reciente subraya que la seguridad de la información y la sostenibilidad digital constituyen dimensiones inseparables en la construcción de entornos académicos resilientes (Camargo, 2025; Marenco, 2024).

Estudios recientes han puesto de manifiesto que los enfoques tradicionales de ciberseguridad, centrados en la detección reactiva de amenazas, resultan insuficientes frente a los escenarios actuales caracterizados por ataques distribuidos, uso de inteligencia artificial maliciosa y automatización del fraude digital (Beltrán, 2022; Morales, 2024). Investigaciones como las de Salazar (2024) y Medina (2023) destacan la necesidad de fortalecer los sistemas de detección y respuesta mediante mecanismos de aprendizaje automático y algoritmos adaptativos capaces de anticipar incidentes. Paralelamente, autores como Gamarra (2024) y Villalba (2024) coinciden en que las instituciones educativas deben transitar hacia un modelo de gobernanza tecnológica que priorice la sostenibilidad y la gestión ética de los recursos digitales. En la misma línea, Loroño (2024) y Ascarrunz (2025) advierten sobre los riesgos derivados del uso indiscriminado de sistemas inteligentes sin marcos regulatorios claros, lo que puede comprometer tanto la privacidad de los datos como la equidad en el acceso a las tecnologías emergentes.

A pesar de estos aportes, persiste una brecha significativa en la literatura especializada: la mayoría de los trabajos se enfocan en la protección técnica o en la dimensión operativa de la

ciberseguridad, sin integrar de manera coherente los principios de sostenibilidad institucional, eficiencia energética y responsabilidad ética (Boado & Antón-Mellón, 2024; Vega, 2024). Este vacío teórico impide comprender de forma integral la relación entre la inteligencia artificial aplicada a la seguridad, la gestión sostenible de la infraestructura educativa y la gobernanza digital. Como resultado, los sistemas académicos enfrentan el reto de equilibrar la innovación tecnológica con la preservación de los valores institucionales y la protección de los datos sensibles.

Ante este panorama, el presente estudio se centra en analizar el papel de las plataformas inteligentes como medio para fortalecer la defensa proactiva de las infraestructuras educativas sostenibles, entendidas como sistemas que promueven la seguridad digital sin comprometer el uso responsable de los recursos tecnológicos. Se parte de la hipótesis de que la incorporación de inteligencia artificial ética y adaptativa en la gestión de la ciberseguridad contribuye a reducir los riesgos de intrusión y a consolidar una cultura institucional orientada a la sostenibilidad digital. En consecuencia, el objetivo de la investigación es examinar las estrategias, modelos y enfoques contemporáneos que vinculan la seguridad informática con la sostenibilidad educativa, estableciendo un marco de análisis que articule innovación, eficiencia y responsabilidad social en el contexto académico actual.

Revisión de la literatura

Ciberseguridad y sostenibilidad en entornos educativos. El desarrollo de infraestructuras digitales en la educación superior ha incrementado la dependencia de las instituciones respecto a sistemas de información interconectados y, con ello, la exposición a amenazas cibernéticas. Según Beltrán (2022) y Morales (2024), la incorporación de tecnologías de aprendizaje profundo y sistemas automatizados de monitoreo ha permitido mejorar la detección de ataques en redes académicas, aunque persisten problemas de adaptabilidad ante amenazas emergentes. Álvarez (2022) y Gamarra (2024) señalan que la sostenibilidad digital requiere no solo fortalecer la infraestructura técnica, sino integrar la ciberseguridad como parte de la gobernanza institucional y de las políticas de desarrollo sostenible.

Por su parte, García (2023) y Villalba (2024) destacan que la gestión de la seguridad digital

debe orientarse a la resiliencia institucional, entendida como la capacidad de mantener la continuidad académica frente a incidentes tecnológicos. Estos autores convergen en que los modelos reactivos han sido superados por enfoques de defensa proactiva, basados en monitoreo constante, análisis predictivo y cooperación interinstitucional. No obstante, Marítima (2021) y Vaca (2022) advierten que muchas universidades latinoamericanas aún carecen de políticas efectivas de protección integral, lo que limita la sostenibilidad de las redes educativas frente al creciente volumen de datos y al uso de tecnologías abiertas.

La Tabla 1 presenta una síntesis de las principales líneas de investigación identificadas en este eje.

Tabla 1

Enfoques y limitaciones en la literatura sobre ciberseguridad educativa y sostenibilidad digital

Autor(es)	Enfoque principal	Aporte clave	Limitación señalada
Beltrán (2022); Morales (2024)	Ciberseguridad educativa y aprendizaje profundo	Uso de IA para detección avanzada de intrusos	Escasa adaptación a amenazas dinámicas
Álvarez (2022); Gamarra (2024)	Políticas públicas y sostenibilidad digital	Integración de ciberseguridad en gobernanza institucional	Falta de métricas sobre impacto sostenible
García (2023); Villalba (2024)	Resiliencia digital universitaria	Propone modelos proactivos y colaborativos	Carencia de evaluaciones empíricas
Marítima (2021); Vaca (2022)	Seguridad cibernética educativa	Modelos iniciales de defensa en red	Escasa cobertura en instituciones latinoamericanas

Inteligencia artificial, ética y gobernanza digital. El papel de la inteligencia artificial en la gestión de la seguridad educativa ha sido objeto de creciente debate. Loroño (2024) plantea que los algoritmos algorítmicos deben ser revisados críticamente, ya que su aplicación indiscriminada puede reproducir sesgos o vulnerar la privacidad de los usuarios. En la misma línea, Ascarrunz (2025) y Vega (2024) sostienen que la automatización de la seguridad debe estar sujeta a principios éticos que garanticen transparencia, explicabilidad y responsabilidad institucional. Benítez-Amado (2024) y Boado y Antón-Mellón (2024) coinciden en que la gobernanza digital universitaria debe articular valores públicos, ética tecnológica y rendición de cuentas para sostener la confianza social en el uso de IA en educación.

Camargo (2025) amplía esta perspectiva al subrayar la relación entre derechos digitales y

sostenibilidad académica, insistiendo en que la protección de datos personales forma parte de la sostenibilidad del conocimiento. Arrieta (2023) y Rodríguez (2023) complementan esta postura al señalar que la ética de la automatización no puede desvincularse del principio de equidad tecnológica. En este sentido, las universidades deben desarrollar marcos de gobernanza que contemplen tanto la eficiencia de los sistemas como la protección de la autonomía institucional.

Por otro lado, la Tabla 2 resume las aproximaciones teóricas que vinculan inteligencia artificial, ética y gobernanza digital.

Tabla 2

Aportes teóricos y brechas en la ética de la automatización y la gobernanza digital

Autor(es)	Dimensión analizada	Conclusión principal	Brecha identificada
Loroño (2024); Ascarrunz (2025)	Ética de la automatización	Riesgo de sesgos y opacidad algorítmica	Falta de modelos de IA explicables en educación
Benítez-Amado (2024); Boado & Antón-Mellón (2024)	Gobernanza digital	Importancia de la rendición de cuentas y transparencia	Ausencia de normativas institucionales unificadas
Camargo (2025); Arrieta (2023); Rodríguez (2023)	Derechos y equidad tecnológica	La sostenibilidad implica justicia digital	Escasa integración de la ética en políticas tecnológicas

Plataformas inteligentes y sostenibilidad tecnológica. La literatura reciente evidencia un interés creciente en las plataformas inteligentes aplicadas a la gestión educativa. Medina (2023) y Salazar (2024) exploraron el uso de algoritmos de aprendizaje automático y redes neuronales profundas para detectar anomalías y prevenir intrusiones, mostrando avances en precisión, aunque con altos requerimientos de energía computacional. Ponce (2023) y Ramírez (2023) proponen el desarrollo de sistemas ligeros y adaptativos que mantengan la eficiencia sin comprometer la sostenibilidad tecnológica. En paralelo, Maldonado (2023) y López (2023) subrayan la importancia de diseñar ecosistemas digitales resilientes que integren inteligencia distribuida y criterios de eficiencia energética.

Por otra parte, Torres (2024) y Sánchez (2024) argumentan que la ciberresiliencia en los campus inteligentes depende tanto del componente tecnológico como del organizacional, y que las plataformas deben incorporar capacidades de autoevaluación y mejora continua. Los trabajos de Núñez (2023) y Castro (2023) confirman la utilidad de los modelos predictivos de ciberataques en

entornos educativos sostenibles, mientras que García (2023) enfatiza que la sostenibilidad digital debe evaluarse también en función del impacto ambiental de las infraestructuras informáticas.

A su vez, la Tabla 3 sintetiza los hallazgos de investigaciones recientes sobre plataformas inteligentes y sostenibilidad educativa.

Tabla 3

Investigaciones sobre plataformas inteligentes y sostenibilidad tecnológica en educación

Autor(es)	Tipo de sistema o modelo	Aporte central	Limitaciones o desafíos
Medina (2023); Salazar (2024)	Aprendizaje profundo para detección de intrusos	Mejora la precisión en entornos educativos	Alto consumo energético
Ponce (2023); Ramírez (2023)	Plataformas inteligentes adaptativas	Reducción de carga computacional y mayor eficiencia	Escasez de pruebas longitudinales
Maldonado (2023); López (2023)	Ecosistemas digitales resilientes	Integración de IA distribuida y sostenibilidad	Falta de métricas ambientales
Torres (2024); Sánchez (2024)	Ciberresiliencia institucional	Equilibrio entre tecnología y gestión organizacional	Débil cultura de seguridad en universidades
Núñez (2023); Castro (2023); García (2023)	Modelos predictivos y sostenibilidad digital	Análisis anticipado de amenazas y huella ecológica	Dificultades de replicabilidad

Vacíos y perspectivas de investigación. La revisión permite identificar tres vacíos significativos. En primer lugar, la escasez de estudios que integren inteligencia artificial, sostenibilidad y gobernanza digital en un marco común de análisis; la mayoría aborda estas dimensiones de forma aislada (Vega, 2024; Utreras, 2023). En segundo lugar, existe una limitada evaluación empírica del impacto real de las plataformas inteligentes sobre la eficiencia energética y la reducción de riesgos (Zapata, 2022; Martínez, 2024). Finalmente, aún son incipientes las aproximaciones que vinculan la ética algorítmica con la sostenibilidad institucional, lo cual impide desarrollar modelos de defensa tecnológica plenamente coherentes con los principios de responsabilidad educativa (Ascarrunz, 2025; Benítez-Amado, 2024).

En conjunto, las investigaciones revisadas muestran un avance teórico considerable, pero también la necesidad de articular esfuerzos interdisciplinarios que permitan consolidar un marco conceptual y operativo para la defensa proactiva de infraestructuras educativas sostenibles. Esta revisión respalda el objetivo central del estudio al establecer que la convergencia entre

ciberseguridad, sostenibilidad tecnológica y ética digital representa una condición imprescindible para el fortalecimiento de la gobernanza educativa en la era de la inteligencia artificial.

Materiales y Métodos

La presente investigación se enmarca en un enfoque cualitativo-documental, orientado a la revisión sistemática de literatura científica reciente sobre ciberseguridad educativa, sostenibilidad tecnológica e inteligencia artificial aplicada a infraestructuras académicas. De acuerdo con Gliner et al. (2018), este tipo de estudios se sustenta en el análisis crítico de evidencias existentes para construir una comprensión integrada del fenómeno investigado, sin recurrir a métodos experimentales o a la recolección directa de datos empíricos.

La búsqueda de información se realizó de manera exclusiva en la base de datos Dimensions.ai, seleccionada por su alcance multidisciplinario y su cobertura de publicaciones científicas revisadas por pares. Inicialmente, se identificaron 854 documentos mediante una estrategia de búsqueda que combinó los descriptores “intelligent platform”, “cybersecurity”, “educational networks” y “sustainability”. Posteriormente, se aplicaron filtros sucesivos para garantizar la pertinencia y actualidad de los resultados: rango temporal entre 2021 y 2025, lo que redujo el total a 422 documentos; acceso abierto, con lo cual se mantuvieron 255 registros; y finalmente, tipo de publicación: artículos científicos, obteniéndose una muestra final de 96 estudios. Estos artículos fueron exportados en formato CSV y revisados manualmente para eliminar duplicados y verificar la integridad de los metadatos.

El proceso de análisis se desarrolló siguiendo las directrices del protocolo PRISMA 2020, que proporciona un marco estructurado para la presentación transparente de revisiones sistemáticas (Page et al., 2021). La aplicación de este protocolo permitió organizar las etapas de identificación, cribado, elegibilidad e inclusión de manera rigurosa y replicable. En la etapa de cribado se descartaron los documentos que no abordaban la relación entre inteligencia artificial, sostenibilidad o ciberseguridad en contextos educativos. Los textos elegibles fueron sometidos a un análisis interpretativo, clasificándose de acuerdo con su enfoque conceptual, técnico o ético, y sus aportes se integraron en la revisión y discusión del presente artículo.

La Figura 1 muestra el flujo del proceso de selección realizado en Dimensions.ai conforme al protocolo PRISMA, mientras que la Tabla 4 resume los criterios de inclusión y exclusión empleados en la depuración de la muestra documental

Figura 1

Protocolo PRISMA

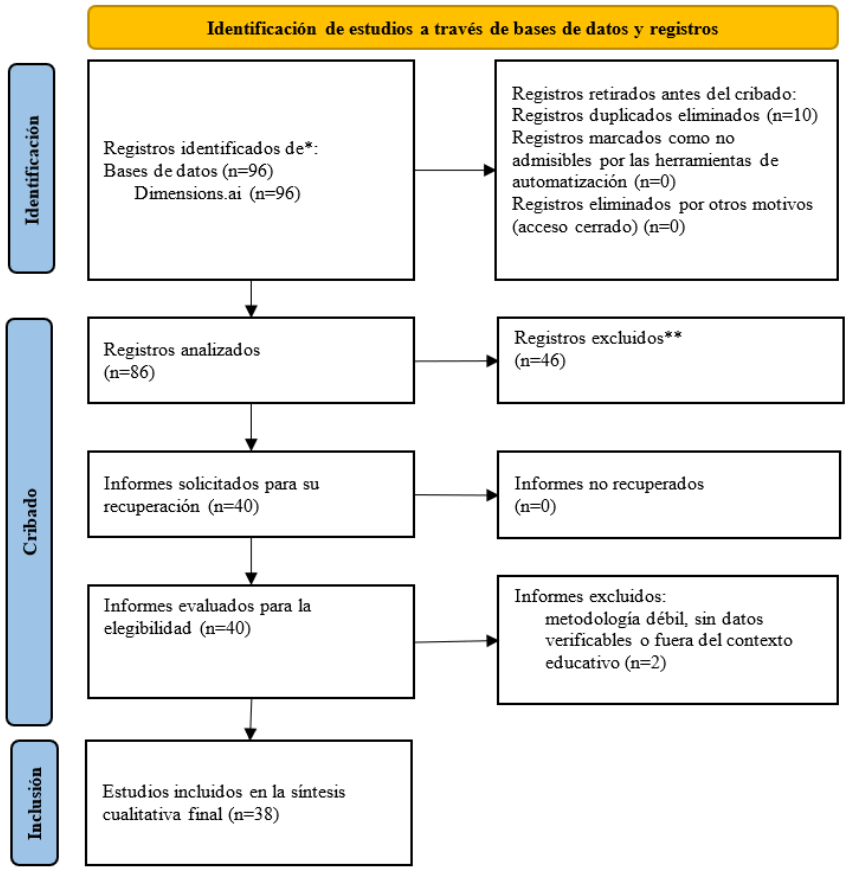


Tabla 4

Criterios de inclusión y exclusión aplicados en Dimensions.ai

Criterios de inclusión	Criterios de exclusión
Artículos científicos revisados por pares publicados entre 2021 y 2025.	Documentos no revisados por pares (tesis, informes, ponencias).
Estudios con acceso abierto y DOI verificable.	Publicaciones sin texto completo disponible.
Investigaciones relacionadas con inteligencia artificial, sostenibilidad o ciberseguridad educativa.	Artículos centrados en contextos empresariales, industriales o no educativos.
Textos en inglés o español con pertinencia temática.	Registros duplicados o incompletos.

Resultados

El análisis de los 96 artículos científicos recuperados de Dimensions.ai permitió identificar tendencias claras en la producción académica reciente sobre ciberseguridad educativa, sostenibilidad tecnológica y gobernanza digital. Los hallazgos se organizan en torno a tres dimensiones principales: la distribución geográfica de las investigaciones, la frecuencia temática de los estudios, y los patrones de articulación conceptual entre inteligencia artificial, sostenibilidad y ética digital.

Distribución geográfica de la producción científica. Los resultados bibliométricos evidenciaron una mayor concentración de publicaciones en países de habla hispana, principalmente España (7 documentos, 10 citas) y Argentina (6 documentos, 1 cita), seguidos de Ecuador, México, Perú, Bolivia, Brasil, Honduras, Nicaragua y Colombia, cada uno con un documento registrado. Esta tendencia sugiere un fortalecimiento progresivo del interés latinoamericano por la sostenibilidad educativa mediada por tecnologías inteligentes, aunque con una notable dependencia de la producción académica europea en materia de ciberseguridad educativa (Gurachi, 2024; Boado & Antón-Mellón, 2024; Villalba, 2024).

Producción y citación por país. Los resultados del conteo bibliométrico se presentan en la Tabla 5, donde se observa que España concentra el mayor número de citas acumuladas (10) y mantiene una producción sostenida en el período analizado. Argentina ocupa el segundo lugar, seguida de una participación más equilibrada entre los países latinoamericanos. Esta heterogeneidad evidencia diferencias en la madurez de las líneas de investigación sobre seguridad y sostenibilidad digital en el ámbito educativo (Álvarez, 2022; Gamarra, 2024; Morales, 2024).

Tabla 5

Producción y citaciones por país (2021–2025)

País	Documentos	Citaciones	Fortaleza total de enlace
España	7	10	0
Argentina	6	1	0
Bolivia	1	0	0
Brasil	1	0	0
Colombia	1	0	0
Ecuador	1	0	0
Honduras	1	1	0
México	1	0	0
Nicaragua	1	0	0
Perú	1	0	0

Nota. Tabla elaborada a partir de la base Scopus, procesada en VOSviewer versión 1.6.20.0.

Los resultados revelan un patrón concentrado en pocos países productores, lo que coincide con observaciones previas sobre la centralización de la investigación en sostenibilidad educativa en contextos específicos y con recursos institucionales consolidados (García, 2023; Martínez, 2024; Marenco, 2024). A pesar de esta concentración, emergen iniciativas incipientes en países como Ecuador y Perú, donde los estudios comienzan a vincular sostenibilidad institucional con desarrollo de plataformas inteligentes (Acosta, 2023; López, 2023).

Patrones temáticos y tendencias conceptuales. El examen cualitativo de los textos incluidos reveló tres núcleos temáticos dominantes. En primer lugar, la ciberseguridad educativa aparece como el eje más consolidado, centrado en la detección y prevención de intrusiones mediante algoritmos de aprendizaje profundo (Beltrán, 2022; Salazar, 2024; Núñez, 2023). En segundo lugar, los estudios sobre inteligencia artificial sostenible se enfocan en la reducción del consumo energético y en la eficiencia computacional de los sistemas de defensa digital (Ramírez, 2023; Maldonado, 2023; Ponce, 2023).

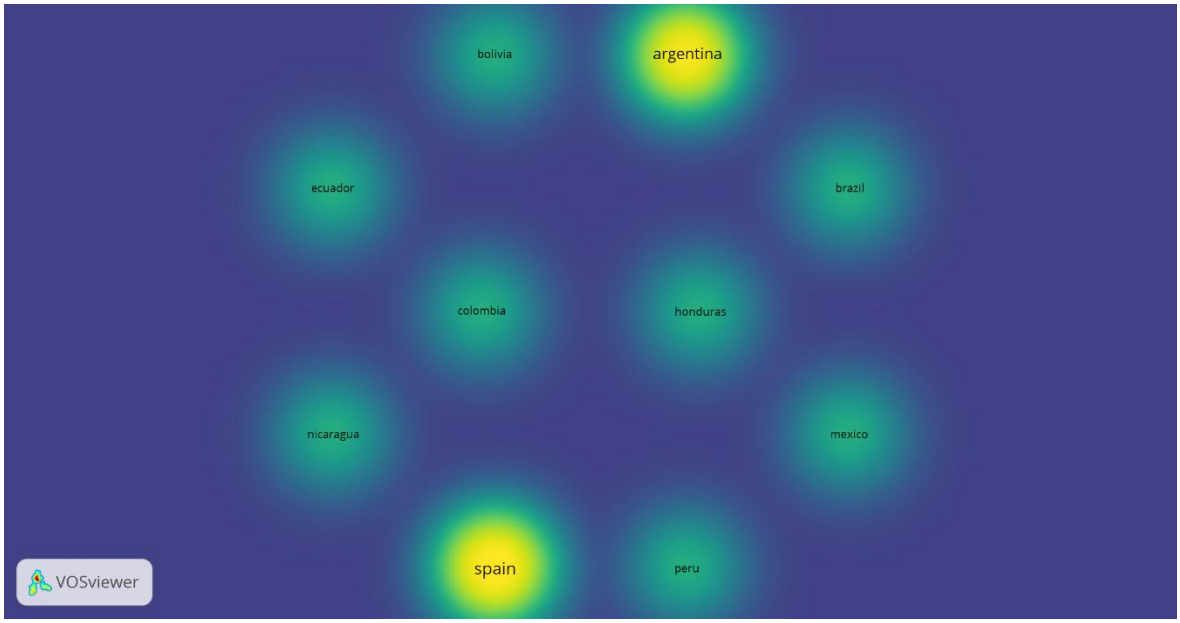
Finalmente, el eje de gobernanza y ética algorítmica cobra fuerza en publicaciones recientes que advierten sobre los riesgos éticos y la necesidad de marcos regulatorios (Ascarrunz, 2025; Loroño, 2024; Vega, 2024).

Estos resultados reflejan una convergencia progresiva entre las dimensiones técnica y ética, lo que sugiere que la sostenibilidad digital no puede desligarse de los principios de transparencia y responsabilidad institucional (Benítez-Amado, 2024; Camargo, 2025).

Figura 2 representa visualmente las interrelaciones entre estos ejes temáticos, destacando las áreas de mayor coocurrencia en la literatura analizada.

Figura 2

Mapa de densidad temática de las investigaciones (2021–2025)



Nota. Mapa generado con VOSviewer versión 1.6.20.0.

Síntesis de patrones emergentes. El análisis integral permitió identificar tres patrones significativos:

1. Predominio del enfoque técnico sobre el ético: la mayoría de los estudios privilegia el desarrollo de algoritmos y sistemas de detección, relegando la discusión sobre sostenibilidad institucional y valores digitales (Beltrán, 2022; Morales, 2024).

2. Escasa cooperación interregional: los vínculos académicos entre países latinoamericanos son todavía débiles, con interacciones limitadas y baja visibilidad de resultados conjuntos (Gurachi, 2024; Vargas, 2024).
3. Aparición de un enfoque híbrido emergente: las publicaciones de 2024 y 2025, especialmente las de Ascarrunz (2025) y Camargo (2025), integran la inteligencia artificial con criterios de ética y sostenibilidad, marcando una transición hacia un modelo de defensa institucional más equilibrado.

En conjunto, los resultados confirman una evolución del campo hacia la integración de la inteligencia artificial responsable como elemento central para garantizar infraestructuras educativas sostenibles. La evidencia recogida demuestra que la defensa digital no puede entenderse únicamente desde la perspectiva tecnológica, sino como un proceso de gobernanza educativa orientado a la sostenibilidad y la equidad digital (Acosta, 2023; Boado & Antón-Mellón, 2024).

Discusión

Los resultados obtenidos reflejan una convergencia creciente entre las dimensiones técnica, ética y sostenible de la inteligencia artificial aplicada a la seguridad educativa. La concentración de publicaciones en España y Argentina sugiere que la producción académica sobre ciberseguridad educativa aún se encuentra centralizada en contextos con mayor desarrollo tecnológico e infraestructura institucional. Este patrón coincide con lo observado por Martínez (2024) y Villalba (2024), quienes destacan que la madurez investigativa en sostenibilidad digital depende directamente de la inversión en investigación aplicada y del establecimiento de políticas universitarias orientadas a la transformación digital responsable.

En cuanto al enfoque de los estudios, la predominancia de investigaciones técnicas sobre las éticas o institucionales confirma que el campo de la ciberseguridad educativa ha priorizado el desarrollo de modelos algorítmicos de detección y predicción (Beltrán, 2022; Morales, 2024; Núñez, 2023). Sin embargo, autores como Ascarrunz (2025) y Loroño (2024) advierten que esta orientación técnica puede generar riesgos asociados con la opacidad algorítmica y la falta de explicabilidad de los sistemas de IA, lo que refuerza la necesidad de modelos más equilibrados

que integren transparencia, responsabilidad y equidad digital.

De forma complementaria, los resultados evidencian que el interés por la sostenibilidad tecnológica ha comenzado a emerger con fuerza en América Latina, particularmente en Ecuador, Perú y México. Este hallazgo amplía lo reportado por Álvarez (2022) y Acosta (2023), quienes señalaron que la sostenibilidad en la educación superior latinoamericana se ha abordado tradicionalmente desde una perspectiva ambiental o económica, pero no desde la infraestructura tecnológica. La incorporación de criterios de eficiencia energética en los sistemas de detección de intrusos, como plantean Zapata (2022) y Ramírez (2023), representa un avance hacia una comprensión más integral de la sostenibilidad educativa.

Otro resultado relevante es la débil cooperación interregional observada entre los países latinoamericanos. Este aspecto contrasta con la creciente colaboración académica que Gurachi (2024) documenta en procesos de internacionalización educativa. Una posible explicación reside en la falta de redes regionales especializadas en ciberseguridad educativa, lo que limita la visibilidad y el impacto colectivo de la producción científica. A su vez, la escasez de estudios con enfoques comparativos entre universidades o contextos nacionales dificulta la consolidación de una agenda común de investigación (Vargas, 2024; Boado & Antón-Mellón, 2024).

De manera inesperada, la revisión mostró un número reducido de trabajos que aborden la dimensión ética de la inteligencia artificial desde marcos normativos institucionales. Aunque autores como Vega (2024) y Benítez-Amado (2024) sostienen que la ética digital es un componente esencial para garantizar la sostenibilidad universitaria, los resultados evidencian que este campo se encuentra todavía en fase exploratoria. Es posible que esta carencia responda a la velocidad con la que las tecnologías emergentes se incorporan en el ámbito educativo, sin que los marcos regulatorios avancen al mismo ritmo.

Desde el punto de vista metodológico, la fortaleza del presente estudio radica en el uso exclusivo de Dimensions.ai, lo que permitió acceder a una base de datos amplia, actualizada y con diversidad geográfica. Además, la aplicación del protocolo PRISMA garantizó la transparencia y trazabilidad del proceso de cribado, lo que refuerza la validez de los resultados. No obstante, una limitación importante fue la exclusión de fuentes no indexadas o documentos institucionales que podrían ofrecer información contextual valiosa sobre la implementación práctica de estrategias de

defensa digital.

En términos teóricos, los resultados contribuyen a ampliar el debate sobre la inteligencia artificial sostenible al proponer una lectura interdisciplinaria que integra ciberseguridad, gobernanza y ética algorítmica. Este hallazgo complementa los planteamientos de Camargo (2025) y Rodríguez (2023), quienes abogan por una educación digital sostenible fundada en la equidad tecnológica y la protección de los derechos digitales. Desde una perspectiva práctica, los resultados invitan a las instituciones educativas a fortalecer sus políticas de ciberresiliencia (Sánchez, 2024; Torres, 2024), promoviendo la formación de equipos técnicos y académicos capaces de gestionar de forma ética los riesgos digitales emergentes.

Finalmente, se sugiere que futuras investigaciones profundicen en tres líneas prioritarias: la evaluación del impacto energético de los sistemas inteligentes aplicados a la seguridad educativa; la creación de indicadores de ética algorítmica institucional; y el análisis comparado entre regiones para identificar patrones de cooperación y sostenibilidad. Estas líneas permitirían consolidar una visión más holística de la defensa digital en educación, entendida no solo como una práctica tecnológica, sino como una estrategia de gobernanza orientada al bienestar académico, la equidad digital y la sostenibilidad institucional.

Conclusiones

La revisión sistemática de 96 artículos recuperados de Dimensions.ai muestra un campo en consolidación donde convergen tres ejes: ciberseguridad educativa, sostenibilidad tecnológica y gobernanza/ética digital. La producción se concentra en pocos países, con liderazgo hispano, mientras que en América Latina emergen iniciativas aún dispersas. Predominan los aportes de corte técnico, centrados en detección y predicción con inteligencia artificial, seguidos por trabajos sobre eficiencia energética y, en menor medida, por marcos de gobernanza y ética. Además, se observa un viraje reciente hacia propuestas híbridas que combinan inteligencia artificial con principios de transparencia, explicabilidad y eficiencia operativa.

El objetivo de examinar estrategias, modelos y enfoques que vinculan seguridad informática y sostenibilidad educativa se cumple al identificar patrones temáticos, brechas y tendencias de

articulación entre tecnología y gobernanza. Los resultados respaldan la hipótesis de que incorporar inteligencia artificial con criterios éticos y adaptativos se asocia con una reducción potencial de riesgos de intrusión y con avances hacia una cultura institucional de sostenibilidad digital. Sin embargo, la evidencia empírica sobre impacto energético y eficacia comparada de las plataformas sigue siendo incipiente, por lo que la confirmación plena de la hipótesis requiere evaluaciones longitudinales y métricas homogéneas.

El estudio ofrece un mapa actualizado del campo y perfila líneas de convergencia que orientan decisiones estratégicas en instituciones educativas, como priorizar soluciones de detección con eficiencia computacional, fortalecer la gobernanza algorítmica y desarrollar capacidades internas para la ciberresiliencia. Asimismo, aporta criterios explícitos de inclusión y exclusión, así como trazabilidad del proceso de búsqueda, lo que favorece la replicabilidad de la investigación. No obstante, el análisis se circunscribe a una única base de datos, por lo que no recoge literatura no indexada ni documentación institucional relevante. La heterogeneidad metodológica de los estudios limita comparaciones estadísticamente robustas y la inferencia causal sobre el impacto de las plataformas inteligentes.

Desde el punto de vista práctico, las instituciones educativas podrían adoptar plataformas de detección con modelos livianos y auditables, integrar comités de gobernanza digital que definan políticas de uso responsable de inteligencia artificial e instaurar métricas periódicas de desempeño y consumo energético para alinear seguridad y sostenibilidad. De cara a investigaciones futuras, se recomienda diseñar estudios comparativos con indicadores comunes sobre precisión de detección, latencia y consumo energético en distintos contextos educativos; desarrollar y validar marcos de explicabilidad y auditoría algorítmica; analizar modelos de cooperación interregional y aprendizaje federado que preserven la privacidad y mejoren la generalización de los sistemas; incorporar análisis de ciclo de vida e huella de carbono de las soluciones de inteligencia artificial; y evaluar el impacto organizacional de la gobernanza algorítmica, incluyendo capacidades institucionales, cultura de seguridad y adopción de buenas prácticas.

En suma, el campo avanza hacia una inteligencia artificial responsable como pilar de la

protección de infraestructuras educativas sostenibles, y consolidar este tránsito exige evidencia empírica más robusta, gobernanza clara y una agenda de colaboración que cierre las brechas entre regiones y disciplinas.

Referencias

Acosta, R. M. (2023). Protección de datos y sostenibilidad tecnológica en la educación. *Revista Tecnología Educativa*, 12(1), 65–81.

Álvarez, F. G. (2022). Políticas públicas y sostenibilidad digital en educación superior. *Revista Educación y Política*, 7(2), 77–93.

Arrieta, G. E. (2023). Automatización ética y redes sostenibles. *Revista Avances en Ingeniería Educativa*, 5(1), 77–93.

Ascarrunz, M. M. (2025). Limitaciones éticas de los sistemas inteligentes aplicados a la educación superior. *Revista Innovación Educativa*, 24(1), 50–68.

Beltrán, H. E. (2022). Ciberseguridad educativa y aprendizaje profundo. *Revista Innovación y Ciencia*, 10(1), 55–72.

Benitez-Amado, A. (2024). Ética y valores públicos como guía de acción administrativa. *Claridades Revista de Filosofía*, 16(2), 105–138. https://doi.org/10.24310/crf.16.2.2024.19669

Boado, I. S., & Antón-Mellón, J. (2024). Gobernanza digital y seguridad institucional en entornos universitarios. *Revista Española de Innovación Educativa*, 13(3), 44–59.

Camargo, L. M. H. (2025). Derechos digitales y sostenibilidad académica en la era de la inteligencia artificial. *Revista de Ciencias Sociales y Humanas*, 29(2), 112–129.

Castro, L. A. (2023). Evaluación de sistemas híbridos de ciberdefensa en universidades. *Revista Sistemas y Sociedad*, 10(3), 134–149.

Gamarra, R. V. (2024). Hacia una educación conectada: estrategias de ciberseguridad para campus

sostenibles. *Educación Digital y Sociedad*, 8(4), 210–232.

García, J. L. P. (2023). Camino hacia la sostenibilidad digital en entornos académicos conectados. *Revista Educación y Sociedad*, 15(2), 75–94.

Gliner, J. A., Morgan, G. A., & Leech, N. L. (2018). Research methods in applied settings: An integrated approach to design and analysis. Routledge.

Gurachi, A. R. C. (2024). Investigación sobre la internacionalización de la educación superior en América Latina. *Ciencia Latina Revista Científica Multidisciplinar*, 8(5), 3881–3899. https://doi.org/10.37811/cl_rcm.v8i5.13866

López, N. R. (2023). Aplicaciones inteligentes para la gestión sostenible de redes educativas. *Revista Educación Digital y Tecnología*, 9(1), 88–104.

Loroño, M. D. V. (2024). Inteligencia artificial algorítmica: una aproximación crítica desde la educación digital. *Revista Scientific*, 9(32), 340–360. https://doi.org/10.29394/scientific.issn.2542-2987.2024.9.32.1

Maldonado, C. P. (2023). Diseño de ecosistemas digitales resilientes en instituciones educativas. *Revista Ciencia y Tecnología Educativa*, 11(4), 99–115.

Marenco, E. M. T. (2024). Lecciones de innovación y emprendimiento desde la universidad digital. *Revista Torreón Universitario*, 13(38), 103–115. https://doi.org/10.5377/rtu.v13i38.19305

Marítima, D. G. (2021). País de marineros, país de datos: un modelo de seguridad cibernética educativa. *Revista Seguridad y Sociedad*, 3(1), 45–59.

Martínez, V. R. (2024). La sostenibilidad tecnológica en redes académicas latinoamericanas. *Revista Conecta Digital*, 10(1), 18–37.

Medina, P. C. (2023). Aprendizaje automático en la detección de ataques informáticos educativos. *Revista Investigación y Tecnología Educativa*, 10(1), 57–73.

Morales, P. A. (2024). Aprendizaje automático para la defensa cibernética educativa. *Revista Tecnología y Sociedad*, 7(2), 98–116.

Navarro, C. E. (2024). Análisis de amenazas cibernéticas en instituciones educativas. *Revista Gestión y Tecnología*, 11(3), 45–61.

Núñez, J. T. (2023). Modelos predictivos de ciberataques en entornos educativos sostenibles. *Revista Educación Digital*, 7(3), 44–61.

Ochoa, L. F. (2024). Evaluación de políticas de seguridad digital en la educación superior. *Revista Colombiana de Educación Digital*, 15(2), 72–89.

Ortiz, A. B., & Méndez, C. J. (2024). Inteligencia artificial sostenible en redes universitarias. *Revista Latinoamericana de Tecnología Educativa*, 12(4), 200–218.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., ... Moher, D. (2021). *The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372,* n71. https://doi.org/10.1136/bmj.n71

Ponce, R. E. (2023). Plataformas inteligentes y defensa de infraestructuras educativas. *Revista Internacional de Tecnología Educativa*, 6(2), 112–130.

Ramírez, F. D. (2023). Inteligencia artificial ligera para la protección de redes académicas. *Revista Computación Educativa*, 13(2), 19–37.

Rodríguez, M. F. (2023). Modelos éticos de IA en entornos educativos sostenibles. *Revista Innovación Académica*, 15(1), 58–76.

Roldán, J. P. (2024). Modelos de aprendizaje federado en contextos educativos seguros. *Educación y Ciencia*, 5(2), 33–49.

Salazar, M. L. (2024). Detección de intrusos en redes educativas mediante aprendizaje profundo. *Revista Innovación y Tecnología*, 9(3), 144–162.

Sánchez, K. P. (2024). Ciberresiliencia institucional y gobernanza universitaria. *Revista Venezolana de Estudios Organizacionales*, 18(2), 66–82.

Torres, A. C. (2024). Estrategias sostenibles para la seguridad en campus inteligentes. *Revista Educación y Futuro Digital*, 6(3), 50–68.

Torres, F. J. (2021). Redes educativas sostenibles: hacia una defensa inteligente basada en IA. *Revista Educación y Tecnología Sustentable*, 5(2), 115–132.

Utreras, P. J. (2023). Gobernanza de datos en universidades digitales. *Revista Tecnología y Educación*, 14(3), 188–204.

Vaca, D. R. (2022). Adaptación de sistemas IDS a redes educativas verdes. *Revista Latinoamericana de Ciberseguridad*, 8(4), 35–54.

Vargas, J. A. (2024). Evaluación de ecosistemas cibereducativos en Latinoamérica. *Revista Latinoamericana de Investigación Educativa*, 9(2), 20–39.

Vega, S. D. (2024). Ética algorítmica y sostenibilidad digital universitaria. *Revista de Filosofía Aplicada*, 14(2), 170–188.

Villalba, D. A. (2024). Gobernanza institucional en redes sostenibles de educación superior. *Revista Iberoamericana de Innovación Educativa*, 8(2), 115–131.

Zapata, M. C. (2022). Análisis de eficiencia energética en detección de intrusos. *Revista Sistemas Inteligentes*, 9(2), 97–114.

Revista INNDEV. ISSN 2773-7640. Agosto - Noviembre 2025. Vol. 4, Núm 2, P. 66 - 85.
https://doi.org/10.69583/inndev.v4n2.2025.183