

Artículo Revisión

Modelos de inteligencia artificial para la detección predictiva de riesgos de ciberseguridad en entornos educativos digitales

Artificial Intelligence Models for the Predictive Detection of Cybersecurity Risks in Digital Educational Environments

Juan Carlos Barco Quiñonez^{1*}  

¹Universidad Estatal de Milagro, Milagro - Ecuador

***Autor de correspondencia:** Juan Carlos Barco Quiñonez 

Recibido: 28-07-2026

Revisado: 18-08-2026

Aceptado: 07-09-2026

Publicado: 29-09-2026

Cómo citar este artículo: Barco Quiñonez, J. C. . (2026). Modelos de inteligencia artificial para la detección predictiva de riesgos de ciberseguridad en entornos educativos digitales. *Educational Regent Multidisciplinary Journal*, 3(2), 1-16. <https://doi.org/10.63969/df80hs86>

RESUMEN

La consolidación de los entornos educativos digitales ha incrementado la interdependencia entre plataformas de aprendizaje, sistemas académicos, redes institucionales, servicios en la nube y dispositivos conectados, ampliando simultáneamente la exposición a riesgos de ciberseguridad. Frente a esta situación, la inteligencia artificial ofrece capacidades para procesar grandes volúmenes de información, reconocer patrones, detectar anomalías y anticipar señales asociadas con posibles amenazas. El análisis se orientó a examinar los enfoques de inteligencia artificial abordados en la producción científica especializada para la detección predictiva de riesgos en entornos educativos digitales, considerando características, aplicaciones, variables, capacidades y limitaciones. Se desarrolló bajo un enfoque cualitativo, descriptivo y documental, mediante el protocolo PRISMA 2020 para la selección y análisis de publicaciones especializadas. Los hallazgos identificaron enfoques supervisados, no supervisados, semisupervisados, aprendizaje profundo, detección de anomalías y predicción. Su alcance depende de la calidad de los datos, representatividad, generalización e interpretación de las señales detectadas.

Palabras clave: Inteligencia artificial; ciberseguridad; detección predictiva; aprendizaje automático; entornos educativos digitales.

ABSTRACT

The consolidation of digital educational environments has increased the interdependence between learning platforms, academic systems, institutional networks, cloud services and connected devices, while simultaneously expanding exposure to cybersecurity risks. In response to this situation, artificial intelligence offers capabilities for processing large volumes of information, recognising patterns, detecting anomalies and anticipating signals associated with potential threats. The analysis examined the artificial intelligence approaches addressed in specialised scientific literature for the predictive detection of cybersecurity risks in digital educational environments, considering their characteristics, applications, variables, capabilities and limitations. A qualitative, descriptive and documentary approach was adopted, using the PRISMA 2020 protocol to select and analyse specialised publications. The findings identified supervised, unsupervised and semi-supervised approaches, deep learning, anomaly detection and predictive techniques. Their scope depends on data quality and representativeness, as well as on the ability of the approaches to generalise and interpret the detected signals.

Keywords: Artificial intelligence; cybersecurity; predictive detection; machine learning; digital educational environments.

1. INTRODUCCIÓN

La consolidación de los entornos educativos digitales ha transformado la forma en que se desarrollan los procesos de enseñanza, gestión académica, comunicación institucional y acceso a recursos de información. Plataformas virtuales, sistemas de gestión del aprendizaje, servicios en la nube, repositorios digitales, redes institucionales y dispositivos conectados conforman infraestructuras cada vez más interdependientes, en las que se generan y procesan grandes cantidades de información académica, administrativa y personal. Esta creciente interconexión amplía las posibilidades de acceso y disponibilidad de los servicios educativos, pero también incrementa la exposición frente a amenazas capaces de comprometer la integridad, confidencialidad y disponibilidad de los recursos digitales. Ante esta realidad, la inteligencia artificial adquiere especial relevancia por su capacidad para analizar grandes volúmenes de datos, reconocer relaciones complejas, identificar desviaciones de comportamiento y establecer patrones asociados con situaciones potencialmente riesgosas. Los modelos de aprendizaje automático y aprendizaje profundo permiten, en este sentido, ampliar las capacidades convencionales de supervisión y detección al incorporar procedimientos orientados al reconocimiento de anomalías y a la identificación anticipada de señales vinculadas con posibles incidentes de ciberseguridad.

La creciente dependencia de las instituciones educativas respecto de infraestructuras digitales ha configurado escenarios en los que múltiples servicios, usuarios y dispositivos interactúan de manera permanente dentro de una misma arquitectura tecnológica. Plataformas de aprendizaje, sistemas de información académica, mecanismos de autenticación, redes inalámbricas, aplicaciones colaborativas, servidores y servicios de almacenamiento concentran operaciones que requieren protección frente a accesos indebidos, código malicioso, suplantación de identidad, extracción de credenciales, interrupción de servicios y diferentes modalidades de intrusión. Esta diversidad tecnológica dificulta mantener una vigilancia uniforme sobre todos los eventos generados, especialmente cuando las amenazas pueden desarrollarse de manera progresiva y presentar señales iniciales poco perceptibles. El desafío trasciende la identificación posterior de un incidente, pues requiere reconocer patrones de comportamiento que puedan advertir condiciones de riesgo antes de que estas produzcan alteraciones significativas en los servicios, la información o la continuidad de las actividades educativas.

Las dificultades se intensifican debido a la variabilidad inherente a los entornos educativos digitales, donde estudiantes, docentes, personal administrativo y sistemas automatizados generan comportamientos tecnológicos diferentes según sus funciones, horarios, dispositivos y necesidades de acceso. Esta heterogeneidad reduce la efectividad de mecanismos sustentados exclusivamente en reglas rígidas, debido a que una modificación legítima en el comportamiento de un usuario puede presentar características similares a una actividad potencialmente maliciosa. Paralelamente, la aparición de amenazas emergentes, modificaciones de ataques conocidos y estrategias destinadas a evadir los mecanismos convencionales plantea la necesidad de disponer de modelos capaces de adaptarse a patrones complejos y cambiantes. En este escenario, la inteligencia artificial ofrece alternativas para analizar tráfico, registros de actividad, eventos de autenticación y otras fuentes de información mediante técnicas de clasificación, detección de anomalías y aprendizaje de patrones. Sin embargo, su utilización también plantea interrogantes relacionados con la calidad y representatividad de los datos, el desequilibrio entre clases, la selección de variables relevantes, la interpretabilidad de las predicciones, la generación de falsos positivos y la capacidad de los modelos para mantener un desempeño adecuado ante situaciones que no estuvieron presentes durante su entrenamiento.

El aprendizaje automático ha adquirido una presencia creciente en el campo de la ciberseguridad debido a su capacidad para procesar grandes cantidades de información y reconocer relaciones que pueden resultar difíciles de establecer mediante procedimientos sustentados exclusivamente en reglas predefinidas. Esta evolución ha favorecido el desarrollo de modelos orientados a clasificar eventos, identificar comportamientos atípicos y reconocer patrones

asociados con actividades potencialmente maliciosas. Merino et al. (2026) examinan diferentes técnicas de minería de datos y aprendizaje automático aplicadas a la detección de intrusiones, considerando los algoritmos utilizados, las características de los datos y las condiciones que pueden afectar su desempeño. Este planteamiento permite comprender que la efectividad de un modelo depende de la interacción entre el método de aprendizaje, las variables seleccionadas y la calidad de la información disponible. Dentro de los entornos educativos digitales, esta consideración resulta relevante debido a la diversidad de registros generados por plataformas de aprendizaje, redes institucionales, sistemas de autenticación y dispositivos conectados.

Durante la evolución de los sistemas de detección de intrusiones se ha producido una ampliación progresiva de los mecanismos destinados a reconocer comportamientos anómalos. Los procedimientos tradicionales pueden identificar determinadas amenazas cuando estas coinciden con patrones previamente registrados, pero presentan mayores dificultades frente a comportamientos desconocidos o modificaciones de ataques existentes. Peizhi (2025) examinan diferentes técnicas de detección y señalan la importancia de los enfoques basados en anomalías para reconocer desviaciones respecto de los patrones considerados normales. Esta orientación resulta particularmente significativa en las instituciones educativas, donde la actividad digital presenta una elevada variabilidad debido a las diferencias entre perfiles de usuarios, horarios, dispositivos, aplicaciones y tipos de interacción. Bajo estas condiciones, identificar un comportamiento potencialmente riesgoso requiere distinguir entre variaciones legítimas y alteraciones que puedan representar una amenaza para los recursos institucionales.

Diversas familias de algoritmos han sido incorporadas al análisis de problemas relacionados con la clasificación, predicción y reconocimiento de patrones en sistemas digitales. Cada aproximación responde de manera diferente a las características de los datos, por lo que la selección del modelo constituye una decisión metodológica vinculada con el tipo de información disponible y la finalidad del análisis. Salas et al. (2026) examina distintas categorías de algoritmos de aprendizaje automático y sus posibilidades de aplicación, destacando la importancia de relacionar las características del problema con el procedimiento computacional seleccionado. Desde esta perspectiva, los modelos supervisados pueden utilizar registros previamente clasificados, mientras que los métodos no supervisados permiten explorar estructuras presentes en datos sin etiquetar; asimismo, los enfoques semisupervisados pueden aprovechar conjuntos que combinan ambas condiciones. Esta diversidad amplía las posibilidades para analizar riesgos en infraestructuras educativas donde no siempre existe información histórica completamente categorizada.

Un enfoque basado en inteligencia artificial permite integrar diferentes procesos de análisis orientados a transformar los registros digitales en información relevante para la seguridad. El procesamiento de datos, el aprendizaje automático, la detección de anomalías y la identificación de patrones pueden funcionar de manera complementaria para caracterizar comportamientos que requieren una valoración adicional. Sánchez et al. (2026) proponen una concepción de inteligencia de seguridad sustentada en datos, en la cual los modelos inteligentes contribuyen al reconocimiento de anomalías, la identificación de intrusiones y el análisis de comportamientos vinculados con amenazas. Esta perspectiva adquiere interés para los entornos educativos porque permite desplazar el análisis desde la simple identificación de incidentes hacia la interpretación de señales que pueden preceder a una alteración de los servicios digitales. Los registros de autenticación, tráfico de red, accesos a plataformas y utilización de recursos pueden constituir fuentes relevantes para estudiar patrones asociados con condiciones potencialmente riesgosas.

Las arquitecturas de aprendizaje profundo han ampliado las posibilidades para representar relaciones complejas entre múltiples características de los datos, especialmente cuando las estructuras presentes en la información resultan difíciles de identificar mediante procedimientos convencionales. Las redes neuronales profundas pueden construir representaciones sucesivas a partir de los registros disponibles y reconocer relaciones que no necesariamente son evidentes mediante técnicas tradicionales. Quirumbay et al. (2022) estudian arquitecturas de aprendizaje profundo aplicadas a la detección de intrusiones y muestran el interés de estas aproximaciones para analizar características relacionadas con el comportamiento de las redes. Su utilización exige, sin embargo, considerar factores como el volumen de información necesario para el entrenamiento, la capacidad computacional requerida, la posibilidad de

sobreajuste y la dificultad para explicar determinadas predicciones. Estas condiciones son especialmente relevantes cuando se analiza su posible aplicación en instituciones educativas, debido a que los patrones de utilización tecnológica pueden diferir considerablemente de aquellos presentes en infraestructuras empresariales o industriales.

Los conjuntos de datos empleados para entrenar y evaluar modelos de inteligencia artificial constituyen un componente determinante dentro del análisis de ciberseguridad. Un algoritmo puede presentar indicadores elevados de desempeño cuando trabaja con información bien estructurada y representativa, pero sus resultados pueden variar cuando los datos contienen desequilibrios, registros insuficientes o características que no reflejan las condiciones reales de funcionamiento. Cruz et al. (2026) revisan diferentes conjuntos de datos empleados en sistemas de detección de intrusiones y destacan la importancia de sus características para valorar adecuadamente el comportamiento de los modelos. La distribución entre tráfico legítimo y malicioso, la diversidad de ataques, la actualización de los registros y la correspondencia entre los datos experimentales y los escenarios reales influyen en la capacidad de generalización. Para las instituciones educativas, esta consideración adquiere especial importancia porque sus patrones de actividad pueden estar condicionados por calendarios académicos, perfiles de usuarios y dinámicas propias de los servicios educativos digitales.

Frente a la transformación constante de las amenazas, resulta necesario valorar hasta qué punto los modelos de inteligencia artificial pueden mantener su capacidad de reconocimiento cuando las condiciones de los datos cambian. Los algoritmos aprenden determinadas relaciones a partir de la información utilizada durante su entrenamiento; por ello, la aparición de comportamientos significativamente diferentes puede reducir su capacidad para clasificar correctamente nuevas observaciones. Bernal et al. (2025) identifican la detección de ataques desconocidos y las estrategias de evasión como desafíos relevantes para los sistemas de detección de intrusiones. Esta situación adquiere particular importancia en los entornos educativos digitales, donde la incorporación de nuevas plataformas, dispositivos, servicios en la nube y modalidades de acceso puede modificar progresivamente los patrones de actividad. Por esta razón, el análisis de un modelo no debería limitarse a sus métricas obtenidas sobre un conjunto específico, sino considerar también su capacidad de generalización, estabilidad y respuesta ante escenarios que presentan características diferentes de aquellas observadas durante el entrenamiento.

Una orientación preventiva de la ciberseguridad requiere ampliar el análisis desde la identificación de eventos ya producidos hacia la interpretación de señales que puedan anticipar condiciones de riesgo. Bajo esta perspectiva, los modelos inteligentes pueden contribuir al establecimiento de relaciones entre variables técnicas, secuencias de actividad y modificaciones en los patrones de comportamiento, generando información susceptible de ser utilizada para valorar escenarios potencialmente adversos. Espinoza et al. (2025) relacionan esta evolución con una inteligencia de seguridad basada en datos, donde la inteligencia artificial participa en la transformación de registros digitales en información útil para reconocer anomalías y analizar amenazas. Este planteamiento permite considerar la detección predictiva como una dimensión complementaria a los mecanismos convencionales de seguridad, especialmente cuando se pretende identificar señales tempranas antes de que un comportamiento alcance una condición crítica. En el ámbito educativo, esta línea de desarrollo resulta relevante para examinar qué modelos presentan características apropiadas para interpretar la variabilidad de los usuarios, procesar grandes volúmenes de información y reconocer patrones que puedan asociarse con riesgos emergentes.

Inteligencia artificial y aprendizaje automático en ciberseguridad

Desde una perspectiva computacional, la inteligencia artificial comprende un conjunto de técnicas orientadas al procesamiento avanzado de información, reconocimiento de patrones, identificación de relaciones y generación de inferencias a partir de grandes volúmenes de datos. Su incorporación al ámbito de la seguridad digital permite analizar registros procedentes de redes, servidores, dispositivos, aplicaciones, plataformas y sistemas de autenticación, especialmente cuando la cantidad de eventos dificulta una supervisión exclusivamente manual. López et al. (2019) señalan que estas técnicas pueden emplearse para reconocer comportamientos, detectar anomalías y analizar posibles amenazas mediante procedimientos capaces de transformar datos heterogéneos en información relevante para la

protección de infraestructuras digitales. Dentro de las instituciones educativas, su utilidad se relaciona con la posibilidad de integrar múltiples fuentes de actividad tecnológica y reconocer asociaciones que difícilmente podrían identificarse mediante reglas estáticas. Esta capacidad favorece una aproximación más amplia a las condiciones que preceden o acompañan determinados incidentes, al considerar simultáneamente variables relacionadas con usuarios, dispositivos, accesos, comunicaciones y servicios digitales.

Dentro de este marco, el aprendizaje automático permite construir procedimientos computacionales capaces de identificar regularidades en conjuntos de datos y utilizarlas posteriormente para clasificar observaciones, reconocer comportamientos, detectar desviaciones o efectuar estimaciones. Su aplicación en seguridad informática comprende el análisis de tráfico de red, registros de acceso, procesos de autenticación, comunicaciones entre dispositivos y eventos generados por diferentes sistemas. Martínez et al. (2018) describen diversas técnicas de minería de datos utilizadas para la detección de intrusiones y destacan la importancia de relacionar el procedimiento seleccionado con las características de la información disponible y con la finalidad concreta del análisis. Esta relación resulta esencial porque el desempeño de una técnica no depende exclusivamente de su formulación matemática, sino también de la calidad de los registros, la selección de variables, la representatividad de las observaciones y las condiciones en que se generan los eventos. En instituciones educativas, tales factores adquieren especial importancia debido a la coexistencia de múltiples perfiles de usuario, dispositivos, plataformas y formas de interacción digital.

Cuando las bases de datos contienen categorías previamente establecidas, el aprendizaje supervisado permite establecer relaciones entre las características de cada observación y una clase conocida, facilitando posteriormente la asignación de categorías a nuevos registros. Este procedimiento puede emplearse para distinguir actividad legítima de comportamientos potencialmente maliciosos, reconocer diferentes tipos de intrusión o clasificar eventos de acuerdo con patrones previamente identificados. Su funcionamiento requiere información suficientemente representativa y etiquetas consistentes, debido a que errores de clasificación durante el entrenamiento pueden trasladarse a las predicciones posteriores. También adquiere importancia la distribución de las categorías, puesto que una presencia reducida de determinados eventos puede dificultar su reconocimiento frente a una cantidad considerablemente mayor de actividades normales. En instituciones educativas, esta situación exige considerar la diversidad de comportamientos legítimos, ya que las variaciones asociadas con horarios académicos, periodos de evaluación, cambios de dispositivo o incorporación de nuevos servicios pueden modificar sustancialmente los patrones habituales de actividad digital.

Cuando las observaciones disponibles no poseen categorías previamente asignadas, el aprendizaje no supervisado permite explorar su estructura interna mediante procedimientos orientados a encontrar agrupaciones, relaciones y desviaciones respecto de determinados patrones. Esta aproximación adquiere relevancia en escenarios donde no existe un inventario completo de amenazas o donde pueden aparecer comportamientos que no corresponden exactamente con categorías conocidas. Santillan et al. (2026) reconocen la detección de anomalías como una aproximación relevante dentro de los sistemas de detección de intrusiones, particularmente porque permite identificar actividades que se apartan de las condiciones consideradas normales. Su aplicación puede facilitar el examen de registros de autenticación, tráfico, accesos y utilización de servicios sin requerir una clasificación previa de todas las posibles situaciones de riesgo. Sin embargo, una desviación estadística no constituye por sí misma una confirmación de una amenaza, debido a que determinadas variaciones pueden responder a cambios legítimos en la dinámica institucional. Por ello, la interpretación de las anomalías debe considerar las características operativas y académicas del entorno donde se generan.

Modelos avanzados y detección de anomalías

A partir de arquitecturas neuronales compuestas por múltiples niveles de procesamiento, el aprendizaje profundo permite construir representaciones complejas de los datos y reconocer relaciones que pueden resultar difíciles de identificar mediante procedimientos convencionales. Su aplicación en seguridad informática se ha extendido hacia tareas relacionadas con la clasificación del tráfico, reconocimiento de patrones, análisis secuencial e identificación de

comportamientos atípicos. Alhasnawi et al. (2026) examinan el empleo de arquitecturas profundas para la detección de intrusiones y destacan su utilidad en escenarios que requieren procesar múltiples características asociadas con la actividad de las redes. No obstante, estas estructuras demandan cantidades considerables de información, capacidad computacional y procedimientos adecuados de entrenamiento y validación. También pueden presentar dificultades relacionadas con el sobreajuste y la interpretación de sus predicciones. En instituciones educativas, tales condiciones deben valorarse junto con las características de la infraestructura disponible y la variabilidad de las actividades digitales, debido a que un desempeño elevado sobre determinados registros no garantiza necesariamente una adecuada generalización ante situaciones diferentes.

Una dimensión estrechamente relacionada con la identificación de amenazas corresponde a la detección de anomalías, cuyo propósito consiste en reconocer observaciones, secuencias o comportamientos que presentan diferencias significativas respecto de los patrones considerados habituales. Su importancia radica en la posibilidad de identificar desviaciones que no necesariamente coinciden con amenazas previamente catalogadas, ampliando la capacidad de vigilancia frente a comportamientos emergentes o modificados. Guerrero et al. (2026) sitúan esta aproximación entre las estrategias relevantes para la detección de intrusiones, especialmente cuando se pretende reconocer actividades que se apartan de las condiciones normales de funcionamiento. En los sistemas educativos digitales, las alteraciones pueden expresarse mediante incrementos inusuales de intentos de autenticación, cambios repentinos en los patrones de acceso, utilización atípica de recursos, modificaciones significativas del tráfico o interacciones inusuales con determinadas plataformas. Su interpretación requiere, sin embargo, diferenciar entre una desviación asociada con una posible amenaza y aquellas variaciones legítimas derivadas de actividades académicas, administrativas o tecnológicas extraordinarias.

Predicción de riesgos en entornos educativos digitales

Desde una perspectiva preventiva, la predicción de riesgos de ciberseguridad busca reconocer señales, tendencias y combinaciones de variables que puedan relacionarse con la ocurrencia futura de eventos adversos. Este enfoque amplía el alcance de la detección convencional porque no se limita a determinar si una actividad corresponde a una amenaza existente, sino que procura identificar condiciones precursoras mediante el análisis de información histórica y patrones temporales. Yaranga et al. (2025) destaca la utilidad de las técnicas computacionales basadas en datos para desarrollar tareas de clasificación, predicción y reconocimiento de patrones en escenarios caracterizados por grandes volúmenes de información. La capacidad anticipatoria depende, por tanto, de factores como la disponibilidad de registros históricos, la calidad de las variables, la frecuencia de los eventos, la estabilidad de los patrones y la capacidad de generalización ante situaciones no observadas. Bajo esta perspectiva, evaluar una propuesta predictiva exige considerar no solo su precisión clasificatoria, sino también su capacidad para reconocer señales tempranas y mantener un desempeño consistente cuando las condiciones de la infraestructura digital experimentan modificaciones.

En las instituciones educativas convergen plataformas de aprendizaje, sistemas académicos y administrativos, redes institucionales, servicios de almacenamiento, aplicaciones colaborativas, dispositivos personales y recursos alojados en la nube, configurando una infraestructura digital amplia y heterogénea. Tal diversidad genera numerosos puntos de interacción y una superficie de exposición susceptible de presentar comportamientos diferenciados según el tipo de usuario, dispositivo, servicio y actividad desarrollada. Pérez et al. (2023) destacan la necesidad de considerar las particularidades de los sistemas educativos conectados al examinar sus condiciones de seguridad y exposición digital. Esta diversidad implica que una técnica desarrollada sobre conjuntos de datos generales puede presentar limitaciones cuando se enfrenta a dinámicas propias de una institución educativa. En consecuencia, el análisis de soluciones predictivas debe atender su capacidad para interpretar variaciones legítimas, reconocer comportamientos atípicos y relacionar diferentes fuentes de información sin generar un volumen excesivo de falsas alertas. Esta especificidad permite comprender por qué la detección anticipada de riesgos requiere considerar simultáneamente las características tecnológicas, operativas y conductuales propias de los ecosistemas educativos digitales.

La herramienta metodológica corresponde a una estrategia de análisis documental, orientada a localizar, seleccionar, organizar y examinar producción científica especializada sobre modelos de inteligencia artificial aplicados a la detección predictiva de riesgos de ciberseguridad en entornos educativos digitales. La organización de la información facilita la comparación conceptual entre los estudios seleccionados y permite reconocer tendencias en el empleo de aprendizaje automático, aprendizaje profundo, detección de anomalías y modelos predictivos, sin confundir el análisis de la producción científica con la implementación de un sistema de ciberseguridad.

Analizar los enfoques de inteligencia artificial abordados en la producción científica especializada en relación con la detección predictiva de riesgos de ciberseguridad en entornos educativos digitales, considerando sus características, aplicaciones descritas, variables examinadas, capacidades identificadas y limitaciones señaladas.

La delimitación temática orienta el análisis hacia los enfoques de inteligencia artificial que han sido abordados por la producción científica especializada en relación con la detección predictiva de riesgos de ciberseguridad dentro de entornos educativos digitales. Esta delimitación permite considerar las características de las aproximaciones descritas, las aplicaciones señaladas en las fuentes consultadas, las variables examinadas, las capacidades atribuidas y las limitaciones reconocidas, manteniendo el alcance en el análisis documental y sin plantear el desarrollo, aplicación o implementación de soluciones tecnológicas. En función de esta delimitación, se formula la siguiente pregunta de investigación: ¿Qué enfoques de inteligencia artificial aborda la producción científica especializada en relación con la detección predictiva de riesgos de ciberseguridad en entornos educativos digitales, y qué características, aplicaciones, variables, capacidades y limitaciones se describen en torno a su utilización?

2. METODOLOGÍA

Enfoque y diseño

El estudio se desarrolló bajo un enfoque cualitativo, con alcance descriptivo y diseño documental, orientado al análisis de la producción científica especializada relacionada con los enfoques de inteligencia artificial para la detección predictiva de riesgos de ciberseguridad en entornos educativos digitales. Este planteamiento permitió examinar las características conceptuales y metodológicas descritas en las publicaciones seleccionadas, así como las aplicaciones, variables, capacidades y limitaciones asociadas con las diferentes aproximaciones de inteligencia artificial. El análisis se circunscribió a la producción académica disponible en las fuentes consultadas, sin contemplar el desarrollo, entrenamiento, aplicación o validación de modelos de inteligencia artificial en instituciones educativas.

Estrategia de búsqueda

La recuperación documental se efectuó mediante búsquedas estructuradas en Scopus, SciELO, Latindex, Relacyt, Dialnet y Google Scholar, complementadas con otras fuentes académicas pertinentes para ampliar la identificación de publicaciones relacionadas con inteligencia artificial y ciberseguridad en escenarios educativos digitales. Se emplearon términos en español e inglés y operadores booleanos AND y OR, combinando expresiones como inteligencia artificial, machine learning, deep learning, cybersecurity, cybersecurity risk, anomaly detection, predictive detection, educational environments y digital education. La estrategia priorizó documentos cuya temática presentara correspondencia directa con la detección, identificación, análisis o predicción de riesgos de ciberseguridad mediante enfoques de inteligencia artificial.

Criterios de inclusión y exclusión

Los criterios de inclusión comprendieron publicaciones científicas y académicas vinculadas directamente con inteligencia artificial y detección o predicción de riesgos de ciberseguridad en entornos educativos digitales; documentos que describieran características, aplicaciones, variables, capacidades o limitaciones de los enfoques examinados; trabajos con información suficiente para realizar un análisis documental; y publicaciones correspondientes al periodo temporal definido para la búsqueda. Se excluyeron registros duplicados, documentos sin relación temática directa, publicaciones centradas exclusivamente en sectores diferentes al educativo cuando sus aportes no guardaban correspondencia con la pregunta de investigación, trabajos sin acceso al contenido necesario

para su valoración y documentos que abordaban inteligencia artificial o ciberseguridad sin establecer una relación pertinente con la detección o predicción de riesgos.

Procedimiento de selección mediante PRISMA 2020

La identificación y selección de las publicaciones se efectuó siguiendo las directrices de PRISMA 2020, con el propósito de garantizar trazabilidad en cada etapa del proceso documental. Las búsquedas iniciales permitieron identificar 156 registros procedentes de las bases y fuentes académicas seleccionadas. Posteriormente, se eliminaron 31 registros duplicados, por lo que quedaron 125 documentos para la fase de cribado. La revisión de títulos y resúmenes permitió excluir 72 publicaciones que no presentaban correspondencia suficiente con la temática, manteniéndose 53 documentos para una evaluación más detallada.

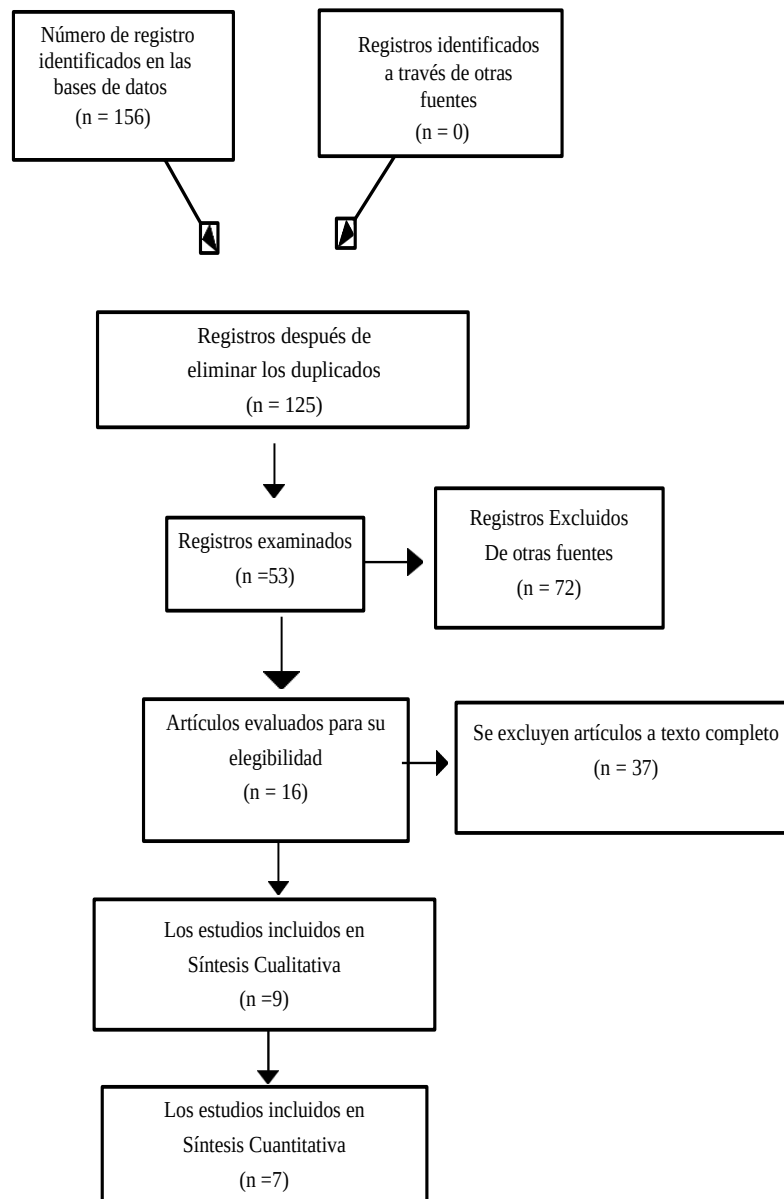
Durante la lectura del texto completo se analizaron los 53 documentos restantes aplicando de manera rigurosa los criterios de inclusión y exclusión. En esta etapa se excluyeron 37 publicaciones debido a falta de correspondencia específica con la detección predictiva de riesgos de ciberseguridad mediante inteligencia artificial, insuficiente información para el análisis, orientación hacia ámbitos no pertinentes o ausencia de relación directa con los entornos educativos digitales. Después de completar este proceso de depuración, se estableció un corpus documental final de 16 publicaciones, las cuales presentaron correspondencia temática, suficiencia informativa y pertinencia respecto de la pregunta de investigación.

Organización y análisis de la información

La organización de los registros y el seguimiento del proceso de selección se realizaron mediante Microsoft Excel, lo que permitió controlar las diferentes etapas de depuración y mantener una organización estructurada de las fuentes recuperadas. El análisis cualitativo se orientó a comparar la información relacionada con los enfoques de inteligencia artificial, aplicaciones descritas, variables consideradas, capacidades predictivas, mecanismos de detección y limitaciones señaladas en las publicaciones seleccionadas. La información organizada permitió reconocer coincidencias, diferencias y tendencias conceptuales entre los documentos examinados, manteniendo el alcance del trabajo en el análisis de la producción científica y sin trasladar sus planteamientos hacia el desarrollo o implementación de una solución tecnológica.

Gráfico 1

Método Prisma



3. RESULTADOS

El análisis de la producción científica seleccionada permitió reconocer una marcada orientación hacia el empleo de técnicas de inteligencia artificial capaces de procesar grandes volúmenes de registros digitales y establecer patrones asociados con comportamientos potencialmente riesgosos. Las publicaciones examinadas describen principalmente aproximaciones basadas en aprendizaje automático, aprendizaje profundo y detección de anomalías, con diferencias en la naturaleza de los datos utilizados y en la finalidad asignada a cada procedimiento. La producción consultada también muestra una transición desde mecanismos centrados exclusivamente en reconocer eventos de seguridad hacia enfoques que buscan identificar señales previas y relaciones temporales asociadas con posibles incidentes. Esta orientación sitúa la capacidad predictiva como un componente relevante para anticipar condiciones de riesgo antes de que produzcan afectaciones sobre los servicios digitales.

Una de las tendencias identificadas corresponde al empleo de técnicas supervisadas para clasificar eventos y diferenciar comportamientos legítimos de actividades potencialmente maliciosas. Los trabajos analizados describen el uso de algoritmos como árboles de decisión, máquinas de soporte vectorial, regresión logística y métodos de ensamble, principalmente cuando se dispone de conjuntos de datos previamente etiquetados. Su aplicación se

relaciona con la identificación de intrusiones, clasificación del tráfico, reconocimiento de patrones de acceso y diferenciación entre comportamientos normales y anómalos. Sin embargo, las publicaciones también señalan que el desempeño de estas aproximaciones depende de la calidad de los datos de entrenamiento, la representatividad de las categorías y el equilibrio entre clases. Cuando determinadas amenazas aparecen con una frecuencia considerablemente menor que las actividades legítimas, la capacidad de reconocimiento puede verse afectada.

Los enfoques no supervisados adquieren relevancia cuando las fuentes de información no cuentan con etiquetas suficientes o cuando existe la posibilidad de que aparezcan comportamientos que no correspondan con amenazas previamente definidas. Las publicaciones revisadas describen procedimientos orientados a encontrar agrupaciones, desviaciones y patrones atípicos mediante técnicas de agrupamiento y detección de anomalías. Esta orientación resulta pertinente para escenarios educativos digitales debido a la elevada variabilidad de las actividades desarrolladas por estudiantes, docentes, personal administrativo y sistemas automatizados. Los registros pueden presentar cambios legítimos relacionados con periodos de evaluación, modificaciones en los horarios de conexión, incorporación de nuevos dispositivos o incremento temporal de determinadas actividades. Por esta razón, la identificación de una anomalía requiere una interpretación contextual que permita diferenciar una desviación estadística de una condición efectivamente asociada con un riesgo de seguridad.

El aprendizaje profundo aparece como una aproximación orientada al tratamiento de información de mayor complejidad y volumen, particularmente cuando se requiere reconocer relaciones no lineales o patrones presentes en secuencias de eventos. Las publicaciones analizadas describen arquitecturas neuronales aplicadas al reconocimiento de tráfico, clasificación de comportamientos, análisis de secuencias y detección de intrusiones. Entre sus principales aportes se encuentra la capacidad para extraer representaciones complejas de los datos sin depender exclusivamente de una selección manual de características. No obstante, también se identifican limitaciones relacionadas con los requerimientos computacionales, la disponibilidad de grandes conjuntos de datos, el riesgo de sobreajuste y la dificultad para interpretar determinadas predicciones. Estas condiciones adquieren especial relevancia cuando se considera su posible pertinencia para infraestructuras educativas con características tecnológicas heterogéneas.

La detección de anomalías constituye una categoría transversal dentro de las aproximaciones examinadas, debido a su capacidad para reconocer desviaciones respecto de patrones considerados habituales. Los estudios revisados relacionan este procedimiento con variables como frecuencia de accesos, volumen de tráfico, intentos de autenticación, comportamiento de dispositivos, conexiones entre servicios y modificaciones en las secuencias de actividad. Su utilidad se encuentra especialmente vinculada con la posibilidad de identificar comportamientos que no han sido previamente clasificados como amenazas. Aun así, las publicaciones coinciden en que una anomalía no representa necesariamente un ataque, puesto que puede originarse por modificaciones legítimas en el comportamiento de los usuarios o en la operación de los servicios. Esta distinción adquiere importancia en instituciones educativas debido a la naturaleza dinámica de sus actividades digitales.

La dimensión predictiva se relaciona principalmente con el uso de registros históricos para identificar combinaciones de variables capaces de anticipar condiciones asociadas con futuros eventos de riesgo. Las publicaciones analizadas muestran que esta perspectiva puede incorporar información temporal, frecuencia de eventos, patrones de acceso, características del tráfico y secuencias de comportamiento. El interés no se limita a reconocer una amenaza cuando ya se encuentra manifiesta, sino a determinar si determinadas señales pueden funcionar como indicadores previos de una condición adversa. En este sentido, la capacidad predictiva depende de la calidad temporal de los registros, la estabilidad de los patrones identificados y la posibilidad de generalizar las relaciones encontradas hacia observaciones diferentes de aquellas utilizadas durante el entrenamiento o análisis.

La especificidad de los entornos educativos digitales constituye otro aspecto relevante identificado en las fuentes examinadas. Las plataformas de aprendizaje, sistemas académicos, servicios administrativos, redes institucionales, aplicaciones colaborativas, recursos en la nube y dispositivos personales generan una superficie digital amplia, caracterizada por múltiples puntos de acceso e interacción. Esta diversidad dificulta establecer un único patrón de

comportamiento normal y exige considerar variables asociadas con diferentes perfiles de usuario y servicios tecnológicos. Los estudios revisados sugieren que la pertinencia de una aproximación de inteligencia artificial depende de su capacidad para procesar esta heterogeneidad sin interpretar automáticamente como amenaza toda modificación respecto de los patrones habituales. La adaptación de los criterios de análisis a las particularidades de las instituciones educativas aparece, por tanto, como una condición relevante para interpretar adecuadamente los riesgos identificados.

Las principales limitaciones descritas en la producción científica se concentran en la disponibilidad y calidad de los datos, la representatividad de los conjuntos utilizados, el desequilibrio entre categorías, la presencia de falsos positivos y falsos negativos, la dificultad para interpretar determinadas predicciones y la capacidad de generalización ante amenazas nuevas. También se reconoce que los resultados obtenidos en conjuntos de datos específicos no necesariamente mantienen el mismo comportamiento cuando cambian las características de la infraestructura, los usuarios o los patrones de actividad. Estas restricciones muestran que el desempeño técnico de una aproximación no constituye por sí solo un criterio suficiente para valorar su pertinencia en escenarios educativos. La interpretación de sus capacidades requiere considerar simultáneamente la naturaleza de los datos, el tipo de amenaza analizada, las características de la infraestructura digital y las condiciones particulares de generación de los registros.

Tabal 1

Principales enfoques de inteligencia artificial identificados en la producción científica

Enfoque	Aplicación descrita	Información analizada	Capacidad identificada	Principales limitaciones
Aprendizaje supervisado	Clasificación de tráfico, intrusiones y eventos de seguridad	Tráfico de red, accesos, autenticaciones, características de conexión	Diferenciar categorías previamente definidas	Dependencia de datos etiquetados y posibles problemas de desequilibrio
Aprendizaje no supervisado	Identificación de comportamientos atípicos y agrupaciones	Patrones de acceso, tráfico, conexiones y actividad digital	Reconocer desviaciones sin etiquetas previas	Posibilidad de confundir variaciones legítimas con amenazas
Aprendizaje profundo	Análisis de patrones complejos y secuencias de eventos	Grandes volúmenes de registros, tráfico y secuencias	Procesar relaciones no lineales y representaciones complejas	Alta demanda computacional y menor interpretabilidad
Detección de anomalías	Reconocimiento de desviaciones respecto del comportamiento habitual	Frecuencia de accesos, autenticaciones, tráfico y actividad	Identificar comportamientos inusuales	Una anomalía no confirma necesariamente una amenaza
Análisis predictivo	Anticipación de condiciones asociadas con futuros riesgos	Datos históricos, variables temporales y patrones de comportamiento	Reconocer señales precursoras de posibles incidentes	Dependencia de la calidad, temporalidad y representatividad de los datos
Enfoques aplicados a entornos educativos	Análisis de riesgos en plataformas, redes y servicios digitales	Usuarios, dispositivos, plataformas, accesos y comunicaciones	Considerar la heterogeneidad de la actividad institucional	Variabilidad de comportamientos y dificultad para establecer patrones normales

Nota. Los enfoques, aplicaciones, variables, capacidades y limitaciones sintetizados se derivan de las características descritas en las publicaciones seleccionadas y corresponden al análisis documental realizado, sin considerar procesos de implementación experimental o validación propia en instituciones educativas.

4. DISCUSIÓN

El análisis realizado permite interpretar que la inteligencia artificial amplía las posibilidades de la ciberseguridad al incorporar procedimientos capaces de reconocer relaciones, clasificar eventos y detectar desviaciones dentro de grandes volúmenes de información digital. Esta capacidad adquiere especial relevancia cuando las amenazas presentan comportamientos variables o no coinciden con patrones previamente establecidos. Merino et al. (2026) señalan que el desempeño de las técnicas de minería de datos y aprendizaje automático se encuentra condicionado por la relación entre los algoritmos empleados, las características de los datos y las condiciones de análisis. Desde esta perspectiva, la selección de una determinada aproximación no debería sustentarse únicamente en su capacidad computacional, sino en la correspondencia entre el procedimiento, las variables disponibles y la naturaleza de los riesgos que se pretende reconocer. En los entornos educativos digitales, esta relación adquiere mayor complejidad debido a la coexistencia de plataformas de aprendizaje, sistemas administrativos, redes institucionales, dispositivos personales y servicios en la nube, cuyos registros pueden presentar comportamientos diferenciados según usuarios, horarios y actividades.

La detección de anomalías representa una dimensión especialmente significativa porque permite reconocer desviaciones que no necesariamente corresponden con categorías de amenazas previamente conocidas. Peizhi (2025) destaca el valor de estos enfoques para identificar comportamientos que se apartan de los patrones considerados normales, mientras que Santillan et al. (2026) sitúan esta capacidad entre las aproximaciones relevantes para el reconocimiento de intrusiones. Esta orientación resulta pertinente para instituciones educativas, aunque requiere una interpretación cuidadosa de las desviaciones identificadas, debido a que un comportamiento inusual no constituye por sí mismo una amenaza. Cambios en los horarios de acceso, incrementos temporales del tráfico, incorporación de nuevos dispositivos o modificaciones en el uso de plataformas pueden responder a dinámicas académicas legítimas. En consecuencia, la utilidad de la detección de anomalías depende de su capacidad para distinguir variaciones propias del funcionamiento institucional de aquellas que presentan características compatibles con situaciones de riesgo. Tal diferenciación constituye una condición importante para reducir falsas alertas y mejorar la interpretación de los eventos identificados.

La capacidad predictiva, por su parte, introduce una dimensión preventiva al desplazar el análisis desde la identificación de acontecimientos ya producidos hacia el reconocimiento de señales y relaciones que puedan asociarse con condiciones futuras de riesgo. Salas et al. (2026) permiten comprender que la selección de algoritmos debe responder a las características de los datos y a la finalidad específica del análisis, mientras que Espinoza et al. (2025) vinculan la inteligencia de seguridad basada en datos con el reconocimiento de anomalías y amenazas a partir de registros digitales. Esta perspectiva adquiere mayor alcance cuando se incorporan variables históricas y secuencias temporales, ya que permiten examinar modificaciones progresivas en los patrones de actividad. Sin embargo, la anticipación no puede desvincularse de la calidad y representatividad de la información utilizada. Cruz et al. (2026) señalan la importancia de las características de los conjuntos de datos empleados en la detección de intrusiones, aspecto que permite interpretar que los indicadores obtenidos mediante información limitada, desactualizada o poco representativa pueden no reflejar adecuadamente condiciones diferentes. Por ello, las capacidades predictivas deben analizarse considerando simultáneamente precisión, generalización, estabilidad y correspondencia de los datos con las dinámicas reales del entorno educativo.

El aprendizaje profundo amplía las posibilidades de procesamiento cuando las relaciones entre variables presentan elevados niveles de complejidad, aunque sus exigencias también introducen restricciones que deben ser consideradas. Quirumbay et al. (2022) destacan el interés de estas arquitecturas para la detección de intrusiones, mientras que Bernal et al. (2025) señalan los desafíos relacionados con ataques desconocidos y estrategias de evasión. Estos planteamientos permiten interpretar que un desempeño favorable bajo determinadas condiciones no garantiza necesariamente una respuesta equivalente ante modificaciones de la infraestructura, incorporación de nuevas tecnologías o aparición de comportamientos no representados durante el entrenamiento. Alhasnawi et al. (2026) también destacan las posibilidades de las arquitecturas profundas para procesar múltiples características de la

actividad de red, aunque su utilización demanda información suficiente, capacidad computacional y procedimientos adecuados de validación. En los entornos educativos digitales, estas condiciones adquieren particular importancia porque la heterogeneidad de usuarios, dispositivos y servicios puede modificar los patrones considerados normales. Pérez et al. (2023) resaltan precisamente la necesidad de considerar las particularidades de los sistemas educativos conectados al examinar sus condiciones de seguridad. En consecuencia, la detección predictiva mediante inteligencia artificial debe entenderse como una aproximación condicionada por la calidad de los datos, la naturaleza de las variables, la capacidad de generalización y las características propias de los ecosistemas educativos digitales, más que como una solución independiente de estas condiciones.

5. CONCLUSIÓN

Los enfoques de inteligencia artificial examinados se articulan principalmente alrededor del aprendizaje supervisado, no supervisado y semisupervisado, el aprendizaje profundo, la detección de anomalías y las técnicas orientadas al reconocimiento de patrones y la predicción. Cada aproximación presenta posibilidades diferenciadas según la estructura de los datos, la disponibilidad de registros categorizados y la naturaleza de los eventos que se pretende reconocer. Esta diversidad muestra que la detección predictiva de riesgos de ciberseguridad no depende de un único procedimiento computacional, sino de la correspondencia entre las características de la información disponible, las variables examinadas y las capacidades específicas de cada enfoque.

La detección de anomalías ocupa una posición relevante debido a su capacidad para reconocer desviaciones respecto de patrones habituales y ampliar la identificación hacia comportamientos que pueden no coincidir con amenazas previamente clasificadas. El análisis predictivo incorpora, además, una dimensión anticipatoria mediante el examen de tendencias, secuencias temporales y relaciones entre variables que pueden asociarse con condiciones futuras de riesgo. Estas capacidades adquieren particular importancia en los entornos educativos digitales, donde confluyen plataformas de aprendizaje, sistemas académicos y administrativos, redes institucionales, dispositivos personales y servicios alojados en la nube.

Entre las variables examinadas destacan los registros de autenticación, tráfico de red, accesos, dispositivos conectados, comunicaciones, utilización de plataformas y patrones de comportamiento. La utilidad de estos datos se encuentra condicionada por su calidad, representatividad, actualización y distribución. El desequilibrio entre categorías, la insuficiencia de registros, los falsos positivos y negativos, el sobreajuste, las dificultades de interpretación y la presencia de amenazas desconocidas constituyen restricciones que inciden directamente en la capacidad de generalización de los enfoques analizados. Por esta razón, los indicadores de desempeño obtenidos bajo determinadas condiciones no deben considerarse suficientes para establecer capacidades equivalentes ante escenarios diferentes. Los entornos educativos digitales presentan particularidades que requieren especial consideración al valorar las posibilidades de detección predictiva. La diversidad de usuarios, dispositivos, horarios, plataformas y modalidades de acceso genera variaciones legítimas en los patrones de actividad que pueden confundirse con comportamientos anómalos. Una aproximación adecuada debe, por tanto, diferenciar las modificaciones propias de la dinámica académica y administrativa de aquellas que presentan características compatibles con situaciones de riesgo. Esta distinción resulta esencial para limitar falsas alertas y favorecer una interpretación más precisa de las señales identificadas.

La inteligencia artificial configura, de este modo, un campo de posibilidades para fortalecer la identificación anticipada de riesgos mediante la articulación de clasificación, reconocimiento de patrones, detección de anomalías y predicción. Sus capacidades se encuentran, no obstante, estrechamente vinculadas con la calidad de los datos, la selección de variables, la representatividad de los registros, la estabilidad de los patrones y las características tecnológicas del entorno educativo. Las limitaciones señaladas muestran que la detección predictiva debe comprenderse como un proceso condicionado por múltiples factores y no como una capacidad automática derivada exclusivamente del uso de algoritmos avanzados. La producción especializada converge así en la necesidad de valorar conjuntamente las

características técnicas de los enfoques de inteligencia artificial y las particularidades de los ecosistemas educativos digitales en los que se pretende interpretar los riesgos de ciberseguridad.

REFERENCIAS BIBLIOGRÁFICAS

- Alhasnawi, B. N., & al, e. (2026). Un análisis exhaustivo de los ciberataques, la ciberseguridad y la gestión energética en redes inteligentes, incluyendo los últimos avances y el aprendizaje automático. *Conversión y gestión de energía: X*, <https://www.sciencedirect.com/science/article/pii/S2590174525006038>.
- Bernal, O. J., & al, e. (2025). Ciberseguridad: Métodos de Defensa Ante Ataques de Infiltraciones. *RIDE. Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-74672025000200926.
- Cruz, S. J., & al, e. (2026). Revisión sistemática sobre identificación de anomalías en el consumo de servicios web masivos mediante técnicas de aprendizaje automático. *Revista Colombiana de Tecnologías de Avanzada*, <https://doi.org/10.24054/rcta.v1i47.4356>.
- Espinoza, O. M., & Quevedo, S. A. (2025). Impacto de la Inteligencia Artificial en los Procesos de Ciberseguridad en la seguridad industrial. Revisión narrativa. *MQRInvestigar*, <https://doi.org/10.56048/MQR20225.9.1.2025.e68>.
- Guerrero, G. K., & al, e. (2026). Modelos de aprendizaje automático en la detección de intrusiones para la protección de entornos educativos digitales. *Revista De Producción, Ciencias E Investigación*, <https://journalprosciences.com/index.php/ps/article/view/940>.
- López, Á. L., & al, e. (2019). Detección de anomalías basada en aprendizaje profundo: Revisión. *Revista Cubana de Ciencias Informáticas*, <https://www.redalyc.org/journal/3783/378365913008/html/>.
- Martínez, A. F., & Hernández, R. J. (2018). Técnicas de minería de datos con software libre para la detección de factores asociados al rendimiento. *REXE. Revista de Estudios y Experiencias en Educación*, <https://www.redalyc.org/journal/2431/243156768012/html/>.
- Merino, V. K., Merino, V. E., Salazar, Á. E., & Yungán, C. J. (2026). Selección de características y evaluación de algoritmos de aprendizaje automático para la detección de ataques PortScan utilizando el conjunto de datos CICIDS2017. *Dominio De Las Ciencias*, <https://dominiodelasciencias.com/ojs/index.php/es/article/view/4954>.
- Peizhi, Y. T. (2025). Garantizando la seguridad del internet de las cosas: Un análisis exhaustivo de los ataques de ransomware, su detección, las contramedidas y las perspectivas de futuro. *Franklin Abierto*, <https://www.sciencedirect.com/science/article/pii/S2773186325000465>.
- Pérez, V. C., & Reeves, H. E. (2023). Educación inclusiva digital: Una revisión bibliográfica actualizada. Las brechas digitales en la educación inclusiva. *Revista Electrónica "Actualidades Investigativas en Educación"*, <https://www.redalyc.org/journal/447/44775742004/html/>.
- Quirumbay, Y. D., & al, e. (2022). Una revisión del aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE (RCTU)*, <https://doi.org/10.26423/rctu.v9i1.671>.
- Salas, M. Á., & al, e. (2026). Algoritmos de aprendizaje automático aplicados en analíticas de aprendizaje en la educación superior. *Revista latinoamericana de estudios educativos*, <https://doi.org/10.48102/rlee.2026.56.2.802>.
- Sánchez, M. K., & al, e. (2026). Modelo de inteligencia artificial para la detección de intrusiones según características de la red y prácticas de los usuarios. *Revista Logos Ciencia & Tecnología*, http://www.scielo.org.co/scielo.php?pid=S2422-42002026000100036&script=sci_arttext.

Santillan, V. R., & Naranjo, S. R. (2026). Detección de intrusiones en redes informáticas mediante aprendizaje automático supervisado. *Saleciana*, <https://dspace.ups.edu.ec/handle/123456789/33051>.

Yaranga, V. I., Trelles, S. J., & Pizarro, P. P. (2025). Integración de la inteligencia artificial y la ciencia de datos para la toma de decisiones en las empresas: un estudio bibliométrico. *Revista InveCom*, https://ve.scielo.org/scielo.php?script=sci_arttext&pid=S2739-00632026000203071.

CONSIDERACIONES ÉTICAS

El presente estudio se llevó a cabo de conformidad con los principios éticos que rigen la investigación con participantes humanos. Antes de la recolección de los datos, el protocolo de investigación fue revisado y aprobado por el comité de ética institucional correspondiente. Todos los participantes fueron informados de manera clara sobre los objetivos del estudio, los procedimientos, las posibles implicaciones y el carácter voluntario de su participación, otorgando posteriormente su consentimiento informado. Durante todo el proceso de investigación se garantizó la confidencialidad de la información, el anonimato de los participantes y el uso exclusivo de los datos recopilados con fines científicos y académicos.

DECLARACIÓN SOBRE EL USO DE INTELIGENCIA ARTIFICIAL (IA)

Los autores declaran que la herramienta de inteligencia artificial generativa ChatGPT fue utilizada exclusivamente para la traducción al idioma inglés y la revisión lingüística del manuscrito. La herramienta no contribuyó a la concepción del estudio, el diseño de la investigación, la recolección de datos, el análisis estadístico, la interpretación de los resultados ni a la elaboración de las conclusiones. Los autores asumen la plena responsabilidad por la originalidad, exactitud, integridad y validez científica del contenido presentado en este manuscrito.

FINANCIAMIENTO

La presente investigación no recibió subvenciones, becas ni apoyo financiero específico por parte de organismos públicos, entidades comerciales u organizaciones sin fines de lucro.

CONFLICTO DE INTERESES

Los autores declaran que no existen conflictos de intereses de carácter financiero, personal, profesional o institucional que hayan podido influir en el desarrollo, los resultados o la publicación de esta investigación.

CONTRIBUCIÓN DE AUTORÍA

Juan Carlos Barco Quiñonez (JCBQ)

Indicar las funciones desempeñadas por cada autor:

Conceptualización: (JCBQ)

Curación de datos: (JCBQ)

Análisis formal: (JCBQ)

Adquisición de fondos: (JCBQ)

Investigación: (JCBQ)

Metodología: (JCBQ)

Administración del proyecto: (JCBQ)

Recursos: No Aplica

Software: (JCBQ)

Supervisión: (JCBQ)

Barco Quiñonez

Validación: (JCBQ)

Visualización: (JCBQ)

Redacción – Borrador original: (JCBQ)

Redacción – Revisión y edición: (JCBQ)