

Artículo Revisión

Ciberseguridad inteligente: aplicación de técnicas de aprendizaje automático para la detección y prevención de amenazas digitales

Intelligent Cybersecurity: Applying Machine Learning Techniques for the Detection and Prevention of Digital Threats

Sofía Barrón Pérez^{1*}  , **Julia Martínez Romero²**  

¹ Tecnológico Nacional de México, CDMX - México

² Tecnológico Nacional de México, CDMX - México

***Autor de correspondencia:** Sofía Barrón Pérez 

Recibido: 22-08-2026

Revisado: 05-09-2026

Aceptado: 26-09-2026

Publicado: 03-10-2026

Cómo citar este artículo: Barrón Pérez, S. ., & Martínez Romero, J. . (2026). Ciberseguridad inteligente: aplicación de técnicas de aprendizaje automático para la detección y prevención de amenazas digitales. *Educational Regent Multidisciplinary Journal*, 3(2), 1-15. <https://doi.org/10.63969/ahzdw418>

RESUMEN

La transformación digital ha incrementado la exposición de sistemas, redes, dispositivos, aplicaciones y datos frente a amenazas capaces de modificar sus características y dificultar su identificación mediante mecanismos convencionales. En este escenario, las técnicas de aprendizaje automático adquieren relevancia por su capacidad para procesar información, reconocer patrones y diferenciar comportamientos asociados con actividades potencialmente maliciosas. El estudio tuvo como finalidad analizar los estudios especializados sobre el uso de estas técnicas en la detección y prevención de amenazas digitales, considerando algoritmos empleados, amenazas examinadas, capacidades de detección, criterios de desempeño, aportes y limitaciones. Se adoptó un enfoque cualitativo, descriptivo y documental, mediante PRISMA 2020 para organizar la identificación, selección y depuración de las fuentes. Los hallazgos muestran aplicaciones de algoritmos supervisados, métodos no supervisados y arquitecturas de aprendizaje profundo en la detección de intrusiones, malware y anomalías. Los modelos supervisados favorecen la clasificación de amenazas previamente caracterizadas, mientras que los procedimientos no supervisados permiten localizar comportamientos atípicos. Las arquitecturas profundas amplían el procesamiento de información compleja y de elevada dimensionalidad. Persisten limitaciones asociadas con la calidad y representatividad de los datos, el desequilibrio entre categorías, los falsos positivos, la interpretabilidad y la evolución constante de las amenazas digitales, condiciones que delimitan las capacidades atribuidas a estas técnicas.

Palabras clave: Inteligencia artificial; aprendizaje automático; ciberseguridad; detección de amenazas; prevención de amenazas digitales.

ABSTRACT

Digital transformation has increased the exposure of systems, networks, devices, applications and data to threats capable of altering their characteristics and making them more difficult to identify through conventional mechanisms. In this setting, machine learning techniques have gained relevance because of their ability to process information, recognise patterns and distinguish behaviours associated with potentially malicious activities. The study aimed to examine specialised studies addressing the use of these techniques for the detection and prevention of digital threats, considering the algorithms employed, threats examined, detection capabilities, performance criteria, contributions and limitations. A qualitative, descriptive and documentary approach was adopted, using PRISMA 2020 to structure the identification, selection and screening of sources. The findings show applications of supervised algorithms, unsupervised methods and deep learning architectures in the detection of intrusions, malware and anomalies. Supervised models facilitate the classification of previously characterised threats, whereas unsupervised procedures

enable atypical behaviours to be identified. Deep learning architectures extend the processing of complex, high-dimensional information. Limitations persist in relation to data quality and representativeness, class imbalance, false positives, interpretability and the continuous evolution of digital threats, all of which constrain the capabilities attributed to these techniques.

Keywords: Artificial intelligence; machine learning; cybersecurity; threat detection; digital threat prevention.

1. INTRODUCCIÓN

La digitalización de las actividades organizacionales, educativas, empresariales y sociales ha ampliado la dependencia de infraestructuras tecnológicas para gestionar información, establecer comunicaciones y ejecutar procesos críticos. Esta interconexión también ha diversificado los puntos susceptibles de explotación por parte de actores maliciosos, cuyas acciones pueden afectar sistemas, aplicaciones, redes, dispositivos y repositorios de datos mediante procedimientos cada vez más variables. La identificación de estas conductas exige capacidades analíticas que trasciendan la comparación con patrones previamente registrados, especialmente cuando las amenazas incorporan modificaciones destinadas a dificultar su reconocimiento. Bajo estas condiciones, las técnicas de aprendizaje automático ofrecen procedimientos para examinar grandes cantidades de información, establecer relaciones entre variables y distinguir comportamientos asociados con actividades legítimas o potencialmente dañinas. Su incorporación a la ciberseguridad ha impulsado nuevas formas de analizar tráfico de red, registros de actividad, archivos, accesos y secuencias de eventos, favoreciendo procesos de identificación más dinámicos. Por ello, resulta relevante examinar la producción científica especializada para determinar cómo se emplean estas técnicas en la detección y prevención de amenazas digitales, qué capacidades se les atribuyen y cuáles son las restricciones que condicionan su aplicación.

La creciente sofisticación de las amenazas digitales ha modificado las condiciones bajo las cuales se desarrollan los procesos de protección informática. Programas maliciosos, ransomware, phishing, intrusiones, ataques de denegación de servicio y mecanismos de evasión pueden presentar comportamientos cambiantes, distribuir sus acciones entre diferentes componentes tecnológicos o alterar sus características para evitar mecanismos de identificación previamente configurados. Las soluciones sustentadas exclusivamente en firmas, reglas predeterminadas o patrones conocidos pueden presentar dificultades ante actividades que no coinciden con registros existentes o que incorporan modificaciones durante su ejecución. Paralelamente, redes, dispositivos, aplicaciones y servicios digitales producen cantidades considerables de registros que contienen información relevante para reconocer actividades irregulares. El desafío no se limita, por tanto, a disponer de mayores cantidades de información, sino a desarrollar procedimientos capaces de transformar esos datos en señales útiles para reconocer posibles amenazas con niveles adecuados de precisión y oportunidad.

El aprendizaje automático introduce una alternativa basada en modelos capaces de extraer regularidades a partir de datos y emplearlas para clasificar eventos, identificar anomalías o reconocer comportamientos asociados con actividades maliciosas. No obstante, su aplicación en ciberseguridad presenta diferencias importantes según el algoritmo empleado, las características de los datos, el tipo de amenaza estudiada, las condiciones de entrenamiento y los criterios utilizados para valorar el desempeño. La presencia de datos desbalanceados, cambios en los patrones de ataque, falsos positivos, falsos negativos, dificultades de interpretación y limitaciones para transferir modelos experimentales hacia infraestructuras reales puede afectar la confiabilidad de las predicciones. También persiste la necesidad de establecer hasta qué punto las técnicas desarrolladas permiten contribuir no solo al reconocimiento de incidentes, sino también a la anticipación y reducción de riesgos. Esta diversidad justifica examinar de manera articulada la producción científica especializada para identificar las técnicas utilizadas, sus ámbitos de aplicación, las capacidades atribuidas a los modelos y las principales restricciones señaladas en relación con la detección y prevención de amenazas digitales.

La utilización del aprendizaje automático en ciberseguridad responde a la necesidad de analizar comportamientos digitales cuya identificación resulta difícil mediante reglas rígidas y patrones previamente establecidos. La transición hacia modelos capaces de aprender relaciones a partir de datos permitió ampliar el análisis de tráfico de red, registros de actividad y eventos asociados con accesos no autorizados, facilitando la diferenciación entre comportamientos legítimos y actividades potencialmente maliciosas. Castillo et al. (2022) señalaron que, aunque el aprendizaje automático había despertado un amplio interés en la detección de intrusiones, su traslado desde entornos experimentales hacia condiciones operativas presentaba dificultades relevantes. Esta consideración resulta importante porque el valor de un modelo no depende únicamente de su capacidad para clasificar correctamente un conjunto de datos, sino también de su comportamiento cuando enfrenta información cambiante, ruido, variaciones en las redes y modalidades de ataque que no estuvieron representadas durante su entrenamiento. La evolución de este campo ha conducido hacia enfoques supervisados, no supervisados y combinados, cada uno con posibilidades diferenciadas para procesar información de seguridad.

Los algoritmos supervisados han constituido una línea importante para la clasificación automatizada de eventos de seguridad, debido a que permiten establecer relaciones entre características observadas y categorías previamente identificadas. Árboles de decisión, máquinas de vectores de soporte, regresión logística, vecinos más cercanos y métodos de ensamble pueden utilizarse para distinguir diferentes clases de tráfico, archivos o comportamientos. La calidad de esta clasificación está estrechamente relacionada con la composición del conjunto de entrenamiento, la selección de atributos y la correspondencia entre los datos utilizados para aprender y las condiciones posteriores de aplicación. Zamora et al. (2021) explican que la capacidad de generalización constituye un aspecto esencial para valorar el comportamiento de un modelo frente a observaciones que no participaron en su construcción. En ciberseguridad, esta propiedad adquiere especial importancia porque las amenazas pueden modificar sus características, utilizar nuevas rutas de propagación o combinar procedimientos previamente conocidos, generando diferencias entre los patrones empleados durante el entrenamiento y aquellos observados durante una intrusión real.

El aprendizaje no supervisado representa una vía distinta para examinar grandes volúmenes de información cuando la clasificación previa de los datos es insuficiente o inexistente. Mediante agrupamiento, reducción de dimensionalidad y detección de anomalías es posible reconocer estructuras que se apartan de las regularidades predominantes y que pueden requerir una revisión especializada. Álvarez (2022) plantean que la detección de anomalías busca identificar observaciones que presentan un comportamiento significativamente diferente respecto de la distribución considerada normal. Esta capacidad resulta particularmente útil cuando se pretende reconocer actividades desconocidas, puesto que no exige disponer anticipadamente de una categoría específica para cada amenaza. Sin embargo, una desviación respecto del patrón habitual no constituye por sí misma una confirmación de actividad maliciosa; puede corresponder a cambios legítimos en el uso de un sistema, modificaciones operativas o situaciones excepcionales. Por esta razón, la definición adecuada de normalidad, la selección de variables y la validación posterior de las alertas constituyen aspectos decisivos para interpretar correctamente las anomalías detectadas.

La evolución hacia arquitecturas de aprendizaje profundo ha modificado la forma de abordar información caracterizada por elevada complejidad, volumen y diversidad estructural. Estas arquitecturas permiten construir representaciones jerárquicas de los datos y reconocer relaciones que pueden resultar difíciles de establecer mediante procesos convencionales de extracción manual de características. Alcívar et al. (2025) explican que el aprendizaje profundo emplea múltiples niveles de representación para extraer estructuras de distinta complejidad a partir de grandes conjuntos de información. Su incorporación a la ciberseguridad ha permitido explorar redes convolucionales para el reconocimiento de patrones, redes recurrentes para el tratamiento de secuencias y arquitecturas híbridas para combinar diferentes tipos de información. No obstante, el incremento de la capacidad representacional también implica mayores exigencias computacionales y dificultades para explicar cómo se produce una determinada clasificación. Esta condición adquiere especial relevancia cuando las decisiones del modelo deben ser examinadas por especialistas responsables de validar una alerta o determinar la naturaleza de un incidente.

El análisis automatizado de software malicioso constituye una de las áreas donde el aprendizaje automático ha experimentado una expansión considerable. Los procedimientos pueden apoyarse en atributos estáticos obtenidos de los archivos, indicadores derivados de su ejecución o secuencias de comportamiento registradas durante la actividad del programa. Esta diversidad permite analizar el malware desde diferentes perspectivas y reducir la dependencia exclusiva de firmas asociadas con muestras conocidas. Una revisión reciente sobre detección de malware mediante aprendizaje profundo señala que los modelos se han aplicado en plataformas como Windows, Linux, Android, iOS y macOS, aunque persisten dificultades relacionadas con la disponibilidad de conjuntos de datos comparables y la interpretación de las decisiones algorítmicas. Catucuago et al. (2022) también destacan las limitaciones asociadas con ataques adversariales y con la capacidad de generalización frente a muestras no observadas. En consecuencia, la detección de código malicioso requiere considerar no solo el rendimiento obtenido con datos conocidos, sino también la capacidad del modelo para conservar su utilidad ante modificaciones, variantes y técnicas diseñadas para evadir los mecanismos de análisis.

Los sistemas de detección de intrusiones han incorporado progresivamente técnicas de aprendizaje automático para examinar flujos de red, conexiones, paquetes, registros y secuencias de actividad. La finalidad consiste en reconocer comportamientos compatibles con accesos no autorizados, explotación de vulnerabilidades o alteraciones respecto de las condiciones habituales de funcionamiento. Diferentes arquitecturas permiten abordar esta tarea mediante clasificación, reconocimiento de anomalías o combinación de ambas perspectivas. Miranda et al. (2021) señalan que los sistemas basados en aprendizaje automático y aprendizaje profundo han sido estudiados mediante diferentes taxonomías, conjuntos de datos y métricas de evaluación, lo que refleja la diversidad metodológica existente en esta área. El desempeño de estos sistemas debe analizarse considerando simultáneamente precisión, exhaustividad, especificidad, puntuación F1 y tasas de error, debido a que una detección excesivamente sensible puede producir numerosas alertas irrelevantes, mientras que un criterio demasiado restrictivo puede dejar sin identificar determinadas actividades maliciosas. La utilidad operativa depende, por tanto, del equilibrio entre capacidad de reconocimiento y generación de alertas que puedan ser gestionadas de manera efectiva.

El incremento de dispositivos conectados, servicios distribuidos y fuentes de registro ha generado condiciones favorables para la aplicación de modelos capaces de procesar información a gran escala. Redes empresariales, infraestructuras en la nube, dispositivos móviles e Internet de las cosas producen datos heterogéneos que pueden contener indicadores relevantes para la identificación de comportamientos anómalos. Torres et al. (2026) destacan el potencial del aprendizaje profundo para automatizar tareas de análisis y clasificación de grandes cantidades de tráfico y datos asociados con actividades de seguridad. Esta capacidad permite explorar mecanismos orientados a priorizar alertas, reconocer secuencias sospechosas y reducir determinadas tareas repetitivas dentro de los procesos de vigilancia digital. Sin embargo, el procesamiento acelerado de información no garantiza por sí mismo una respuesta adecuada, pues los modelos deben mantener niveles aceptables de precisión y estabilidad cuando reciben datos continuos y heterogéneos. La infraestructura de procesamiento, la latencia, la calidad de los registros y la capacidad para distinguir señales relevantes de eventos ordinarios condicionan la utilidad de estas soluciones en operaciones de seguridad.

La evolución de los modelos de aprendizaje automático aplicados a la ciberseguridad exige considerar no solo su capacidad para reconocer amenazas, sino también su resistencia ante modificaciones deliberadas destinadas a alterar las predicciones. Las estrategias utilizadas por los atacantes pueden dirigirse directamente contra los sistemas protegidos y, de manera particular, contra los modelos encargados de clasificarlos, mediante datos manipulados o entradas diseñadas para inducir decisiones incorrectas. Vergara et al. (2026) demostraron que los sistemas de aprendizaje automático pueden presentar vulnerabilidades frente a diferentes modalidades de ataque, lo que evidencia la necesidad de incorporar mecanismos de protección durante las etapas de entrenamiento y funcionamiento. Esta consideración ha favorecido el desarrollo de enfoques basados en aprendizaje continuo, selección pertinente de características, modelos de ensamble, inteligencia artificial explicable y procedimientos

destinados a preservar la privacidad de los datos. A ello se suman dificultades relacionadas con la heterogeneidad de las bases de datos, la interpretabilidad de las predicciones y la resistencia frente a técnicas adversariales capaces de modificar las entradas sin alterar necesariamente su apariencia original. Por consiguiente, la aplicación del aprendizaje automático en ciberseguridad requiere modelos que mantengan un desempeño consistente ante variaciones de las amenazas y que, además de alcanzar niveles adecuados de precisión, proporcionen condiciones de transparencia, robustez, adaptación y confiabilidad para apoyar la identificación y prevención de incidentes digitales.

La construcción de modelos computacionales destinados al análisis de información permite reconocer relaciones, regularidades y comportamientos que no siempre pueden establecerse mediante reglas previamente programadas. En ciberseguridad, esta capacidad posibilita convertir registros de actividad, tráfico de comunicaciones, características de archivos y eventos del sistema en datos susceptibles de procesamiento y clasificación automatizada. Aguilar et al. (2024) sostiene que un sistema mejora su desempeño en una tarea mediante la experiencia obtenida a partir de los datos, lo que vincula el entrenamiento con la capacidad posterior de generar predicciones. Esta concepción permite comprender la incorporación de procedimientos algorítmicos en la identificación de actividades legítimas y potencialmente maliciosas. Su funcionamiento, no obstante, depende de la calidad y representatividad de la información utilizada, puesto que las características presentes en los datos de entrenamiento influyen directamente sobre las relaciones que el modelo logra establecer.

La clasificación basada en información previamente identificada permite establecer correspondencias entre determinadas características y categorías de actividad. Los procedimientos supervisados utilizan ejemplos etiquetados para construir funciones capaces de asignar nuevas observaciones a clases conocidas, circunstancia que favorece su utilización en el reconocimiento de tráfico, archivos y comportamientos asociados con diferentes tipos de amenazas. Ramírez (2020) destacan que la generalización constituye una propiedad esencial de los modelos, ya que su desempeño debe mantenerse ante observaciones que no participaron en el proceso de entrenamiento. Esta condición adquiere particular importancia en seguridad digital debido a las modificaciones que pueden experimentar las amenazas según el sistema afectado, los mecanismos de propagación empleados o las estrategias de evasión utilizadas. La representatividad de los datos, la validación cruzada y el control del sobreajuste adquieren así una función determinante para conservar la capacidad predictiva del modelo.

El análisis de información que no dispone de categorías previamente asignadas ofrece posibilidades distintas para explorar estructuras internas y comportamientos poco frecuentes. Los procedimientos de agrupamiento, reducción de dimensionalidad y análisis de similitudes permiten organizar observaciones según características compartidas y localizar registros que presentan diferencias respecto de las tendencias predominantes. Zecchetto et al. (2021) explican que los métodos no supervisados permiten descubrir estructuras relevantes dentro de conjuntos de datos sin depender necesariamente de etiquetas establecidas con anterioridad. Esta propiedad resulta pertinente para examinar actividades cuya naturaleza todavía no ha sido determinada y para localizar patrones que podrían corresponder con comportamientos inusuales. Una desviación estadística, sin embargo, no constituye por sí misma una confirmación de actividad maliciosa, debido a que también puede originarse en modificaciones legítimas del funcionamiento de un sistema. La interpretación requiere integrar las características del comportamiento detectado con las condiciones específicas de la infraestructura analizada.

La identificación de anomalías se sustenta en la comparación entre determinadas observaciones y una representación previamente establecida del comportamiento esperado. Variables como frecuencia de accesos, volumen de tráfico, duración de conexiones, consumo de recursos o secuencias de comandos pueden utilizarse para determinar desviaciones relevantes dentro de los registros de actividad. Hernández et al. (2022) señalan que los métodos de detección de anomalías buscan localizar patrones que presentan diferencias significativas respecto de las regularidades predominantes en un conjunto de datos. Su aplicación en seguridad digital permite examinar situaciones para las cuales no existen necesariamente antecedentes de clasificación, ampliando la posibilidad de reconocer actividades desconocidas. La principal dificultad reside en distinguir una modificación legítima de una conducta

asociada con riesgo, por lo que la selección de variables, la definición de los parámetros de normalidad y la validación de las alertas adquieren especial importancia.

Desde una perspectiva estadística, la clasificación de eventos requiere establecer relaciones entre un conjunto de características observadas y categorías previamente determinadas. Esta operación puede orientarse a diferenciar comunicaciones legítimas de actividades maliciosas o a reconocer modalidades específicas de ataque mediante indicadores técnicos extraídos de los registros. Rengifo (2021) plantea que el reconocimiento de patrones permite establecer correspondencias entre variables de entrada y categorías de salida mediante modelos estadísticos y probabilísticos. Sobre esta base se han desarrollado aplicaciones que emplean árboles de decisión, máquinas de vectores de soporte, redes neuronales y métodos de ensamble para procesar información relacionada con incidentes de seguridad. La selección de cada procedimiento depende de factores como la naturaleza de los datos, el número de variables, la complejidad del problema, los recursos computacionales disponibles y el nivel de interpretación requerido para respaldar las decisiones generadas.

El desarrollo de arquitecturas neuronales con múltiples niveles de representación ha ampliado las posibilidades para procesar información caracterizada por relaciones complejas. Estas estructuras permiten identificar características directamente a partir de los datos y construir representaciones sucesivas que facilitan el reconocimiento de patrones de elevada dimensionalidad. Rodríguez et al. (2024) explican que el aprendizaje profundo permite obtener representaciones jerárquicas mediante diferentes niveles de procesamiento, favoreciendo su utilización en tareas donde intervienen grandes cantidades de información. En ciberseguridad, las redes convolucionales pueden emplearse para reconocer estructuras presentes en determinadas representaciones de datos, mientras que las arquitecturas recurrentes permiten analizar secuencias y dependencias temporales. Su implementación también plantea exigencias relacionadas con disponibilidad de datos, capacidad computacional, tiempo de entrenamiento y dificultad para interpretar las decisiones generadas por modelos de elevada complejidad.

La valoración del desempeño constituye un componente indispensable para determinar la capacidad real de un modelo de detección. Una clasificación puede producir aciertos al reconocer amenazas o actividades legítimas, pero también errores derivados de falsas alarmas o de amenazas que permanecen sin identificar. Castañeda (2024) señalan que las métricas de evaluación ofrecen perspectivas complementarias sobre el comportamiento de los clasificadores y deben seleccionarse de acuerdo con las características de la tarea. En ciberseguridad, la precisión, sensibilidad, especificidad, exhaustividad, puntuación F1 y tasa de falsos positivos permiten examinar diferentes dimensiones del funcionamiento del sistema. La interpretación conjunta de estos indicadores resulta necesaria debido a que cada tipo de error puede generar consecuencias distintas: una amenaza omitida puede comprometer la seguridad de un sistema, mientras que una cantidad elevada de falsas alarmas puede incrementar la carga de análisis y dificultar la priorización de incidentes relevantes.

La evolución constante de las amenazas digitales exige que los modelos mantengan su capacidad de respuesta frente a modificaciones que alteren las características de los datos observados. Técnicas de evasión, cambios en los patrones de ataque y aparición de nuevas vulnerabilidades pueden generar diferencias entre las condiciones utilizadas durante el entrenamiento y aquellas presentes durante la operación. Álvarez et al. (2021) advierten que la aplicación del aprendizaje automático en sistemas de detección de intrusiones enfrenta dificultades asociadas con la distancia entre los escenarios experimentales y las condiciones reales de funcionamiento. Este planteamiento amplía la valoración de los modelos hacia aspectos como estabilidad, adaptación, calidad de los datos, interpretabilidad y capacidad para responder ante modificaciones del entorno. Una solución de ciberseguridad basada en técnicas inteligentes requiere, por tanto, mantener un equilibrio entre capacidad predictiva y condiciones operativas que permitan utilizar sus alertas dentro de procesos de análisis, validación y respuesta frente a incidentes digitales.

El procedimiento documental permitirá organizar, examinar y sistematizar la producción científica especializada relacionada con la aplicación de técnicas de aprendizaje automático para la detección y prevención de amenazas digitales. La información seleccionada será examinada mediante categorías vinculadas con las técnicas algorítmicas

empleadas, los tipos de amenazas abordadas, los conjuntos de datos utilizados, las métricas aplicadas para valorar el desempeño de los modelos, sus principales aportes y las limitaciones señaladas en cada fuente. Este proceso favorecerá la comparación de los enfoques desarrollados en diferentes trabajos académicos y permitirá reconocer coincidencias, diferencias, tendencias y vacíos relacionados con el uso de modelos computacionales en ciberseguridad. La organización de la información facilitará una interpretación estructurada de los aportes especializados y permitirá establecer qué plantea la producción científica acerca de las capacidades del aprendizaje automático para fortalecer la identificación, anticipación y prevención de amenazas digitales.

Objetivo

Analizar los estudios especializados que abordan el uso de técnicas de aprendizaje automático para la detección y prevención de amenazas digitales, considerando los algoritmos empleados, los tipos de amenazas examinados, las capacidades de detección descritas, los criterios utilizados para valorar el desempeño de los modelos, así como sus principales aportes y limitaciones.

El análisis de los estudios especializados permite delimitar los principales enfoques empleados para abordar la detección y prevención de amenazas digitales mediante técnicas de aprendizaje automático. Esta delimitación considera las características de los algoritmos utilizados, los tipos de amenazas examinados, las capacidades de detección descritas y los criterios empleados para valorar el desempeño de los modelos, además de los aportes y limitaciones señalados en las fuentes consultadas. A partir de estos elementos, se plantea la siguiente pregunta de investigación: ¿Qué plantean los estudios especializados sobre el uso de técnicas de aprendizaje automático para la detección y prevención de amenazas digitales, particularmente en relación con los algoritmos empleados, los tipos de amenazas examinados, las capacidades de detección descritas, los criterios de evaluación, los aportes y las limitaciones identificadas?

2. METODOLOGÍA

El estudio se desarrolló mediante un enfoque cualitativo, con alcance descriptivo y orientación documental, dirigido al análisis de estudios especializados sobre el uso de técnicas de aprendizaje automático para la detección y prevención de amenazas digitales. El proceso de selección y organización de las fuentes se estructuró conforme a las directrices PRISMA 2020, con el propósito de establecer una secuencia ordenada para la identificación, depuración, cribado y selección de los documentos pertinentes. El análisis se centró en los planteamientos, técnicas, algoritmos, tipos de amenazas, criterios de evaluación, aportes y limitaciones descritos en las fuentes seleccionadas.

La estrategia de búsqueda se estableció mediante la combinación de descriptores relacionados con las categorías centrales del estudio: inteligencia artificial, aprendizaje automático, machine learning, ciberseguridad, cybersecurity, detección de amenazas, threat detection, prevención de amenazas, malware, intrusion detection, anomaly detection y digital threats. Los términos se combinaron mediante los operadores booleanos AND y OR para ampliar y, posteriormente, delimitar la recuperación de documentos. La búsqueda se efectuó en Scopus, SciELO, Latindex, Dialnet, Redalyc, Relacyt y Google Scholar, complementándose con otras fuentes académicas especializadas cuando fue necesario localizar documentos directamente relacionados con las categorías de análisis. Se consideraron publicaciones académicas disponibles en español e inglés, priorizando aquellas que presentaran información suficiente para examinar el empleo de técnicas de aprendizaje automático en procesos de detección o prevención de amenazas digitales.

Los criterios de inclusión comprendieron documentos académicos y científicos relacionados directamente con el aprendizaje automático aplicado a la ciberseguridad; publicaciones que abordaran técnicas, algoritmos o modelos destinados a identificar, clasificar, detectar o prevenir amenazas digitales; estudios que describieran las características de las amenazas examinadas; documentos que informaran criterios o métricas de evaluación; y fuentes con información suficiente para analizar aportes y limitaciones. Se excluyeron documentos duplicados, publicaciones sin relación directa con el tema, trabajos centrados exclusivamente en inteligencia artificial sin aplicación a la seguridad digital, documentos que no abordaran técnicas de aprendizaje automático, registros sin acceso al contenido necesario

para su análisis, publicaciones de carácter exclusivamente divulgativo y fuentes cuyo contenido no permitiera responder a la pregunta de investigación.

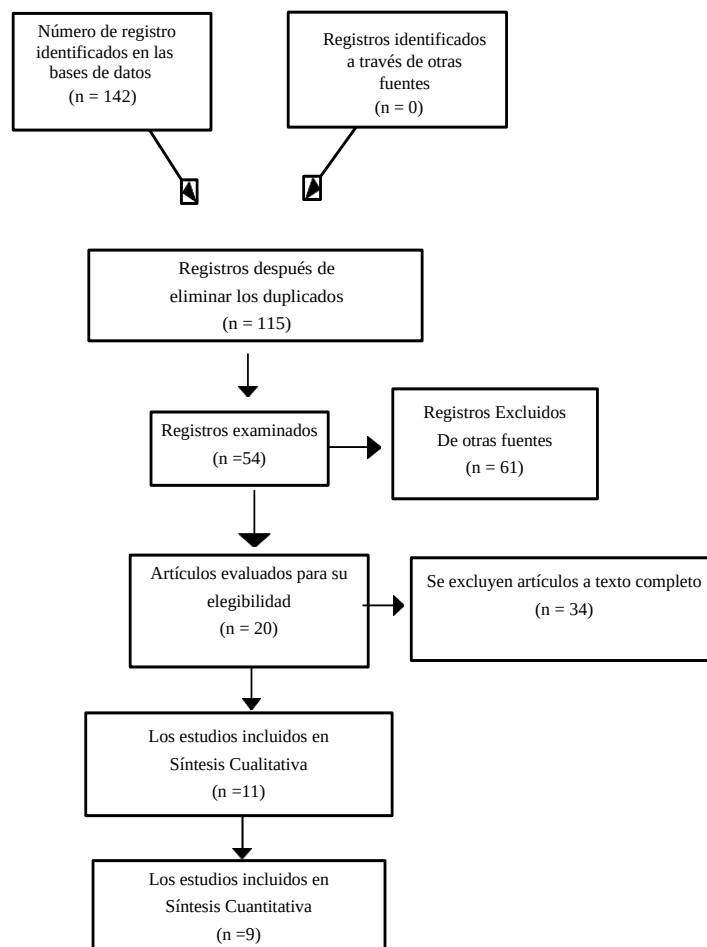
La información recuperada se organizó mediante Microsoft Excel, donde se registraron los datos bibliográficos y las categorías pertinentes para el análisis. La matriz de organización permitió clasificar cada documento según autoría, año de publicación, idioma, técnica de aprendizaje automático, algoritmo empleado, tipo de amenaza abordada, finalidad del modelo, características de los datos considerados, criterios o métricas de evaluación, principales aportes y limitaciones. Esta organización facilitó la comparación cualitativa de los documentos y permitió identificar regularidades, diferencias y tendencias en los enfoques descritos.

El proceso de selección se desarrolló siguiendo las cuatro fases establecidas por PRISMA 2020. En la fase de identificación, se recuperaron 142 registros procedentes de las bases de datos y fuentes académicas seleccionadas. Posteriormente, se eliminaron 27 registros duplicados, por lo que permanecieron 115 documentos para la fase de cribado. Durante esta etapa se revisaron títulos y resúmenes, excluyéndose 61 registros por no presentar correspondencia suficiente con el tema, las variables de análisis o los criterios establecidos. De esta depuración se obtuvieron 54 documentos para la fase de elegibilidad.

En la fase de elegibilidad se realizó una lectura detallada de los 54 documentos disponibles en texto completo. Esta revisión permitió excluir 34 documentos debido a falta de pertinencia temática, insuficiencia de información para el análisis, ausencia de relación directa entre aprendizaje automático y ciberseguridad, o incumplimiento de los criterios de inclusión previamente definidos. Como resultado del proceso, se seleccionaron 20 documentos que cumplieron las condiciones establecidas y conformaron el corpus documental definitivo para el análisis cualitativo.

Gráfico 1

Método Prisma



3. RESULTADOS

La aplicación de técnicas de aprendizaje automático aparece asociada con diferentes formas de detección de amenazas digitales, especialmente mediante procedimientos destinados a reconocer patrones de comportamiento, clasificar actividades maliciosas y localizar desviaciones respecto de determinadas condiciones de normalidad. Entre las aproximaciones descritas se encuentran algoritmos supervisados, métodos de detección de anomalías, redes neuronales y arquitecturas de aprendizaje profundo. Su utilización se relaciona con características específicas de los datos procesados y con la naturaleza de las amenazas que se pretende reconocer, mostrando una diversidad de aplicaciones que abarca desde el tráfico de red hasta archivos, registros de sistemas y secuencias de actividad.

Los algoritmos supervisados se vinculan principalmente con tareas en las que las categorías de actividad legítima y maliciosa se encuentran previamente definidas. Árboles de decisión, máquinas de vectores de soporte, regresión logística, vecinos más cercanos y métodos de ensamble aparecen asociados con la clasificación de tráfico, archivos y eventos de seguridad. Esta capacidad permite diferenciar determinadas clases de comportamiento a partir de características previamente establecidas, aunque su desempeño depende de la correspondencia entre los datos utilizados y las características de las amenazas que posteriormente deben ser reconocidas. Las modificaciones en los patrones de ataque pueden reducir la capacidad de clasificación cuando las nuevas manifestaciones presentan características diferentes de aquellas representadas en los datos disponibles.

La detección de anomalías se relaciona con la identificación de comportamientos que se apartan de los patrones predominantes dentro de los registros digitales. Agrupamiento, reducción de dimensionalidad y otros procedimientos de exploración permiten localizar actividades poco frecuentes sin depender necesariamente de categorías previamente asignadas. Esta característica resulta especialmente pertinente ante comportamientos cuya naturaleza no ha sido determinada con anterioridad, aunque una desviación respecto de la actividad habitual no implica necesariamente una amenaza. Las modificaciones legítimas en el funcionamiento de sistemas, redes o usuarios también pueden generar patrones atípicos y, por ello, producir alertas que requieren interpretación adicional.

Las arquitecturas de aprendizaje profundo muestran aplicaciones vinculadas con información de elevada complejidad y grandes volúmenes de datos. Las redes neuronales convolucionales aparecen relacionadas con el reconocimiento de estructuras presentes en diferentes representaciones de información, mientras que las redes recurrentes se asocian con el procesamiento de secuencias y dependencias temporales. Esta capacidad ha sido utilizada en tareas de detección de intrusiones, clasificación de malware y reconocimiento de patrones de tráfico. Al mismo tiempo, la complejidad de estas arquitecturas se relaciona con mayores requerimientos de procesamiento, disponibilidad de datos y dificultades para explicar de manera transparente las decisiones generadas.

La detección de intrusiones constituye una de las aplicaciones más frecuentes del aprendizaje automático dentro de las fuentes examinadas. Los modelos descritos utilizan características relacionadas con paquetes de red, protocolos, frecuencia de conexiones, duración de sesiones y patrones de tráfico para distinguir actividades normales de comportamientos potencialmente maliciosos. Entre las amenazas abordadas aparecen accesos no autorizados, ataques de denegación de servicio, exploración de redes y diferentes modalidades de actividad intrusiva. La capacidad de reconocimiento se encuentra vinculada con la naturaleza de las variables empleadas y con la similitud entre los patrones representados en los datos y las manifestaciones de las amenazas que se pretende identificar.

La detección de malware presenta aplicaciones orientadas tanto al reconocimiento de características estáticas como al análisis del comportamiento durante la ejecución. Los atributos de archivos, las instrucciones, las llamadas al sistema y las secuencias de comportamiento son utilizados para diferenciar software legítimo de muestras potencialmente maliciosas. Esta diversidad permite abordar distintas manifestaciones del software malicioso, incluidas aquellas que modifican determinadas características para dificultar su identificación. Persisten, sin embargo, dificultades asociadas con la ofuscación, la aparición de nuevas variantes y las modificaciones destinadas a evadir los mecanismos de detección.

La capacidad de discriminación de los modelos se describe mediante indicadores que permiten observar diferentes formas de acierto y error. La precisión, sensibilidad, especificidad, exhaustividad, puntuación F1 y tasa de falsos positivos aparecen entre las medidas utilizadas para caracterizar el comportamiento de los clasificadores y detectores. La interpretación conjunta de estos indicadores permite distinguir entre modelos que identifican correctamente determinadas amenazas y aquellos que generan una cantidad considerable de falsas alarmas o dejan actividades maliciosas sin reconocer. En consecuencia, el desempeño no se reduce a una única medida, puesto que cada indicador representa una dimensión diferente de la capacidad de detección.

Las limitaciones descritas se concentran en aspectos relacionados con la calidad de los datos, el desequilibrio entre categorías, la diversidad de las amenazas y la capacidad de los modelos para responder ante modificaciones de los patrones conocidos. También se señalan dificultades para interpretar arquitecturas complejas y para trasladar directamente determinados desempeños a escenarios con características diferentes de aquellas representadas en los datos utilizados. La evolución de las amenazas introduce una condición adicional, debido a que nuevas variantes de malware, modificaciones en los patrones de intrusión y estrategias de evasión pueden alterar las características sobre las cuales se sustentan las predicciones.

Tabla 1

Técnicas de aprendizaje automático y amenazas digitales identificadas

Enfoque	Aplicación identificada	Eventos abordados
Árboles de decisión	Clasificación de eventos y comportamientos	Intrusiones, tráfico malicioso y actividades anómalas
Máquinas de vectores de soporte	Clasificación de patrones	Malware, intrusiones y tráfico de red
Regresión logística	Clasificación de actividades	Eventos legítimos y potencialmente maliciosos
Métodos de ensamble	Integración de múltiples clasificadores	Intrusiones, malware y tráfico sospechoso
Agrupamiento	Organización de patrones y detección de desviaciones	Actividades anómalas y comportamientos desconocidos
Detección de anomalías	Identificación de comportamientos atípicos	Intrusiones y actividades inusuales
Redes neuronales convolucionales	Reconocimiento de estructuras complejas	Malware y tráfico de red
Redes neuronales recurrentes	Procesamiento de secuencias	Patrones temporales e intrusiones
Aprendizaje profundo	Clasificación y reconocimiento de patrones complejos	Malware, intrusiones y amenazas digitales diversas

Nota. La tabla presenta las principales relaciones identificadas entre las técnicas de aprendizaje automático, sus aplicaciones y las amenazas abordadas en las fuentes examinadas.

Tabla 2

Capacidades de detección y principales limitaciones identificadas

Dimensión	Características identificadas
Reconocimiento de patrones	Identificación de regularidades y comportamientos asociados con actividades legítimas o maliciosas
Detección de anomalías	Localización de desviaciones respecto de patrones predominantes

Dimensión	Características identificadas
Clasificación de amenazas	Diferenciación entre categorías de malware, intrusiones y eventos de seguridad
Detección de amenazas conocidas	Reconocimiento de patrones previamente representados en los datos
Detección de comportamientos desconocidos	Identificación de desviaciones o características no previamente categorizadas
Falsos positivos	Generación de alertas ante actividades legítimas que presentan características atípicas
Falsos negativos	Omisión de determinadas actividades maliciosas
Calidad de los datos	Influencia sobre la capacidad de generalización y precisión de los modelos
Evolución de las amenazas	Necesidad de considerar modificaciones en malware, intrusiones y mecanismos de evasión
Interpretabilidad	Dificultad para explicar decisiones generadas por modelos complejos

Nota. Las categorías sintetizan las capacidades y restricciones descritas en las fuentes examinadas y permiten organizar los principales aspectos asociados con la detección automatizada de amenazas digitales.

4. DISCUSIÓN

La incorporación del aprendizaje automático en ciberseguridad amplía las posibilidades de identificar comportamientos que presentan características asociadas con actividades maliciosas. Su principal aporte se relaciona con la capacidad de procesar múltiples variables y reconocer relaciones que resultan difíciles de establecer mediante reglas estáticas. Esta característica favorece una detección basada en patrones y permite abordar información procedente de tráfico de red, archivos, registros de sistemas y actividades digitales.

Los modelos supervisados muestran especial utilidad en situaciones donde las categorías de interés se encuentran previamente definidas. Su aplicación permite diferenciar comportamientos legítimos y potencialmente maliciosos mediante características previamente establecidas, aunque su capacidad de reconocimiento depende de que las categorías representadas mantengan correspondencia con las nuevas observaciones. Esta condición adquiere importancia ante amenazas que modifican sus características y dificultan la clasificación basada en patrones conocidos. La detección de anomalías aporta una perspectiva diferente al permitir localizar comportamientos que se apartan de las regularidades predominantes sin requerir necesariamente una clasificación inicial. Esta posibilidad resulta relevante frente a actividades cuya naturaleza todavía no se encuentra determinada. Sin embargo, las desviaciones también pueden corresponder con modificaciones legítimas, por lo que la identificación de una anomalía debe diferenciarse de la confirmación de una amenaza.

El aprendizaje profundo amplía las posibilidades de procesamiento ante estructuras de información complejas, particularmente en tareas relacionadas con secuencias, tráfico y características de archivos. Las arquitecturas con múltiples niveles de representación permiten reconocer relaciones que presentan elevada dimensionalidad, aunque esta capacidad se acompaña de mayores exigencias computacionales y dificultades para interpretar las decisiones generadas. La complejidad del modelo adquiere así una relación directa con las condiciones requeridas para aprovechar sus capacidades.

Las aplicaciones orientadas a la detección de intrusiones y malware muestran que las técnicas de aprendizaje automático pueden abordar amenazas con características diferenciadas. En las intrusiones se consideran patrones de tráfico, conexiones y comportamientos de red, mientras que en el malware se examinan atributos estáticos y dinámicos asociados con archivos y procesos. Esta diferenciación confirma que la utilidad de cada aproximación depende de la naturaleza de la información disponible y de las características particulares de la amenaza examinada.

La valoración de las capacidades de detección requiere interpretar conjuntamente diferentes indicadores de desempeño. Precisión, sensibilidad, especificidad, exhaustividad, puntuación F1 y tasa de falsos positivos representan dimensiones distintas del comportamiento de los modelos y permiten identificar situaciones en las que un desempeño aparentemente favorable oculta dificultades en la detección de determinadas clases. Esta consideración resulta especialmente relevante en escenarios donde los errores de clasificación tienen consecuencias diferentes para la seguridad de los sistemas.

Las principales restricciones se relacionan con la representatividad de los datos, el desequilibrio entre categorías, la generación de falsas alarmas y la aparición de comportamientos que no se encuentran suficientemente representados. Estas condiciones pueden limitar la correspondencia entre las capacidades descritas y situaciones diferentes de aquellas consideradas en los datos de cada trabajo. La evolución de las amenazas introduce, además, una variación permanente que dificulta mantener patrones de reconocimiento estables.

La diversidad de aproximaciones muestra que no existe una única técnica capaz de responder de manera uniforme a las diferentes categorías de amenazas digitales. Los procedimientos supervisados, no supervisados y de aprendizaje profundo presentan capacidades diferenciadas y responden a necesidades específicas de clasificación, exploración y reconocimiento de estructuras complejas. Esta diversidad permite comprender el aprendizaje automático como un conjunto de recursos analíticos cuya utilidad depende de la relación entre algoritmo, información disponible y tipo de amenaza.

En este sentido, la aplicación del aprendizaje automático a la ciberseguridad se caracteriza por un equilibrio entre capacidad de reconocimiento y condiciones de uso. Las técnicas permiten ampliar la identificación de patrones, anomalías, intrusiones y comportamientos asociados con malware, pero sus alcances están condicionados por la calidad de los datos, la evolución de las amenazas y la posibilidad de interpretar adecuadamente las alertas generadas. La contribución de estas aproximaciones se encuentra, por tanto, en su capacidad para complementar los mecanismos de detección mediante análisis automatizado de información digital diversa.

5. CONCLUSIÓN

Las técnicas de aprendizaje automático presentan capacidades relevantes para la detección y prevención de amenazas digitales al permitir procesar grandes volúmenes de información, reconocer patrones y diferenciar comportamientos asociados con actividades potencialmente maliciosas. Su utilización comprende tráfico de red, archivos, registros de sistemas y secuencias de actividad, ampliando las posibilidades de identificación automatizada de eventos relacionados con la seguridad digital.

Los algoritmos supervisados se orientan principalmente hacia la clasificación de amenazas previamente caracterizadas, mientras que los procedimientos no supervisados permiten localizar comportamientos atípicos sin depender de categorías definidas inicialmente. Las arquitecturas de aprendizaje profundo amplían el procesamiento de información compleja y de elevada dimensionalidad. Esta diversidad muestra que las capacidades de cada aproximación se relacionan con la naturaleza de los datos, las características de la amenaza y la finalidad específica de la detección.

La detección de intrusiones, el reconocimiento de malware y la identificación de anomalías constituyen aplicaciones relevantes dentro de los enfoques examinados. Las técnicas descritas permiten reconocer patrones de tráfico sospechoso, accesos no autorizados, comportamientos inusuales y características asociadas con software malicioso. Las capacidades de detección presentan variaciones según el algoritmo y las condiciones de información consideradas, por lo que su desempeño debe interpretarse de acuerdo con cada escenario analizado.

La valoración de los modelos requiere considerar diferentes indicadores, debido a que una sola medida no representa todas las dimensiones de su comportamiento. Precisión, sensibilidad, especificidad, exhaustividad, puntuación F1 y tasa de falsos positivos permiten distinguir diferentes relaciones entre aciertos y errores. Esta valoración adquiere especial importancia en ciberseguridad, donde tanto la omisión de amenazas como la generación excesiva de alertas pueden afectar la utilidad de los mecanismos de detección.

Las principales limitaciones se relacionan con la calidad y representatividad de los datos, el desequilibrio entre categorías, la aparición de amenazas con características nuevas y la dificultad para interpretar modelos de elevada complejidad. Estas condiciones restringen la generalización de las capacidades descritas y muestran que el desempeño depende de la correspondencia entre la información utilizada y las características de las amenazas examinadas.

La incorporación del aprendizaje automático a la ciberseguridad configura un campo caracterizado por la diversidad de algoritmos, aplicaciones y capacidades de detección. Su aporte se vincula con la posibilidad de complementar los mecanismos de identificación mediante el procesamiento automatizado de información digital, mientras persisten desafíos relacionados con la adaptación ante nuevas amenazas, la interpretabilidad de los modelos y la calidad de los datos. Estas condiciones permiten comprender que el desarrollo de capacidades inteligentes de ciberseguridad requiere considerar simultáneamente las características algorítmicas, informacionales y dinámicas de las amenazas digitales.

REFERENCIAS BIBLIOGRÁFICAS

- Aguilar, G. F., & Pazos, Y. E. (2024). El Aprendizaje Basado en Problemas como estrategia metodológica para el desarrollo del Pensamiento Crítico. *Revista de estudios y experiencias en educación*, <http://dx.doi.org/10.21703/rexe.v23i53.2658>.
- Alcívar, J. G., & Aguilera, A. J. (2025). Consideraciones legales y constitucionales sobre accidentes de tránsito en Ecuador: Un estudio de revisión. *Prohominum. Revista de Ciencias Sociales y Humanas*, <https://doi.org/10.47606/acven/ph0306>.
- Álvarez, A. O., & Rodríguez, M. L. (2021). La evaluación del desempeño, una nueva herramienta de la cultura de la transparencia aplicada al sector público en México. *Trascender, contabilidad y gestión*, <https://doi.org/10.36791/tcg.v0i18.126>.
- Álvarez, C. L. (2022). Estándar para activar la obligación de comunicar sobre ciberincidentes relevantes en instituciones públicas. *Revista chilena de derecho y tecnología*, <http://dx.doi.org/10.5354/0719-2584.2021.65502>.
- Castañeda, S. W. (2024). Redes neuronales artificiales: una medición de aprendizajes de pronósticos como demanda potencial. *Universidad, Ciencia y Tecnología*, <https://doi.org/10.47460/uct.v27i118.686>.
- Castillo, Y. C., & Coronel, S. I. (2022). Una revisión del aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE (RCTU)*, <https://doi.org/10.26423/rctu.v9i1.671>.
- Catucuago, I. D., & Chugá, Q. R. (2022). El error inexcusable: un freno al abuso mediante la determinación del procedimiento en la legislación ecuatoriana. *Dilemas contemporáneos: educación, política y valores*, <https://doi.org/10.46377/dilemas.v9i.3013>.
- Hernández, V. M., & Berríos, A. F. (2022). Instalación de un proceso de observación de aula: experiencia y desafíos. *Revista de estudios y experiencias en educación*, <http://dx.doi.org/10.21703/0718-5162.v21.n46.2022.024>.
- Miranda, B. S., & Ortiz, B. J. (2021). Los paradigmas de la investigación: un acercamiento teórico para reflexionar desde el campo de la investigación educativa. *RIDE. Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, <https://doi.org/10.23913/ride.v11i21.717>.
- Ramírez, D. J. (2020). El enfoque por competencias y su relevancia en la actualidad: Consideraciones desde la orientación ocupacional en contextos educativos. *Revista Electrónica Educare*, <http://dx.doi.org/10.15359/ree.24-2.23>.

- Rengifo, A. D. (2021). Análisis de reducción de dimensiones para el reconocimiento de actividades físicas humanas usando fusión multimodal. *Ingeniare. Revista chilena de ingeniería*, <http://dx.doi.org/10.4067/S0718-33052021000400717> .
- Rodríguez, J. C., & Alonso, G. S. (2024). Revisión sistemática de la literatura sobre la seguridad digital en estudiantes de educación superior. *Información tecnológica*, <http://dx.doi.org/10.4067/s0718-07642024000400001> .
- Torres, G. N., & Zúñiga, C. M. (2026). Panorama actual de la ciberseguridad: amenazas, legislación y brechas estructurales desde una revisión sistemática. *Revista InveCom*, <https://doi.org/10.5281/zenodo.15605545> .
- Vergara, C. E., & Caballero, M. S. (2026). Metodologías activas en la educación latinoamericana: una revisión sistemática sobre su impacto en el aprendizaje significativo. *Revista InveCom*, <https://doi.org/10.5281/zenodo.16076292> .
- Zamora, E., Sossa, H., & Lugo, S. O. (2021). Reconocimiento robusto de lugares mediante redes neuronales convolucionales. *Computación y Sistemas*, <https://doi.org/10.13053/cys-24-4-3340> .
- Zecchetto, F., & López, M. (2021). Desarrollo Profesional Docente para la Inclusión: Investigación Acción Colaborativa a través de Estudios de Clase en Escuelas Chilenas. *Revista latinoamericana de educación inclusiva*, <http://dx.doi.org/10.4067/S0718-73782021000200067> .

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

Sofía Barrón Pérez (SBP)

Barrón Pérez et al.

Julia Martínez Romero (JMR)

Indicar las funciones desempeñadas por cada autor:

Conceptualización: (SBP)

Curación de datos: (JMR)

Análisis formal: (SBP)

Adquisición de fondos: (JMR)

Investigación: (SBP)

Metodología: (JMR)

Administración del proyecto: (SBP)

Recursos: No Aplica

Software: (SBP)

Supervisión: (JMR)

Validación: (SBP)

Visualización: (JMR)

Redacción – Borrador original: (SBP)

Redacción – Revisión y edición: (JMR)