



**FACULTAD DE INGENIERÍA ARQUITECTURA Y  
URBANISMO**

**ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

**TRABAJO DE INVESTIGACIÓN**

**Revisión sistemática sobre el uso de la Inteligencia  
Artificial para la detección y prevención de fraudes  
financieros**

**PARA OPTAR EL GRADO ACADÉMICO DE BACHILLER  
EN INGENIERÍA DE SISTEMAS**

**Autores**

Mondragon Fernandez Alex

ORCID: <https://orcid.org/0000-0001-8270-392X>

Yarango Farro Darwin Orlando

ORCID: <https://orcid.org/0000-0002-7704-287X>

**Asesor**

Mg. Mejia Cabrera Heber Ivan

ORCID: <https://orcid.org/0000-0002-0007-0928>

**Línea de Investigación**

**Ciencias de la información como herramientas multidisciplinares  
y estratégicas en el contexto industrial y de organizaciones**

**Sublínea de Investigación**

**Nuevas tendencias digitales orientadas al análisis y uso estratégico  
de la información**

**Pimentel – Perú**

**2025**


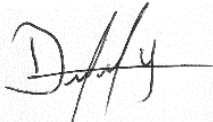
**DECLARACIÓN JURADA DE ORIGINALIDAD**

Quienes suscribimos la **DECLARACIÓN JURADA**, somos **Mondragon Fernandez Alex y Yarango Farro Darwin Orlando** egresados, del programa de estudios de **Ingeniería de Sistemas**, de la Universidad Señor de Sipán S.A.C, declaramos bajo juramento que somos autores del trabajo titulado:

**Revisión sistemática sobre el uso de la Inteligencia Artificial para la detección y prevención de fraudes financieros**

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán (CIEI USS) conforme a los principios y lineamientos detallados en dicho documento, en relación a las citas y referencias bibliográficas, respetando al derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y auténtico.

En virtud de lo antes mencionado, firman:

Mondragon Fernandez Alex	DNI: 60160683	
Yarango Farro Darwin Orlando	DNI: 76680636	

Pimentel, 23 de enero del 2025

## **Dedicatoria**

Dedicamos este trabajo a nuestros padres, hermanos, quienes siempre confiaron en nosotros, apoyándonos en todos los momentos de nuestras vidas y brindándonos un constante ejemplo de perseverancia y superación, sin importar el tiempo que tomara alcanzar nuestros objetivos.

Asimismo, queremos hacer una dedicatoria especial a nuestros docentes, por todas las enseñanzas recibidas a lo largo de nuestra carrera universitaria.

## **Agradecimientos**

Agradecemos a Dios por permitirnos alcanzar una meta más en nuestra vida, otorgándonos constancia, sabiduría y fortaleza para culminar este trabajo de titulación.

A la Universidad Señor de Sipán y a los docentes de la carrera de Ingeniería de Sistemas, quienes supieron impartir los conocimientos necesarios para nuestra formación ética y académica.

De igual manera, agradecemos a nuestros compañeros de estudios, con quienes compartimos experiencias y que fueron un soporte y refuerzo a lo largo de nuestra vida estudiantil.

## Índice

Dedicatoria.....	3
Agradecimientos .....	4
Índice de tablas, figuras y fórmulas .....	6
Resumen .....	7
Abstract.....	8
I. INTRODUCCIÓN.....	9
1.1. Realidad problemática.....	9
1.2. Formulación del problema .....	11
1.3. Hipótesis.....	12
1.4. Objetivos .....	12
1.5. Teorías relacionadas al tema.....	12
II. MÉTODO DE INVESTIGACIÓN .....	19
III. RESULTADOS .....	26
IV. DISCUSIÓN Y CONCLUSIONES.....	62
V. REFERENCIAS.....	65
ANEXOS.....	73

## Índice de tablas, figuras y fórmulas

Figura 1. Uso de cadenas para la búsqueda de artículos en Scopus .....	22
Figura 2. Uso de cadenas para la búsqueda de artículos ScienceDirect.....	22
Figura 3. Diagrama de flujo PRISMA .....	26
Figura 4. Técnicas IA más efectivas.....	57
Figura 5. Ventajas y Limitaciones de técnicas de IA .....	58
Figura 6. Casos de impacto positivo de la IA .....	61
Tabla 1. Criterios de elegibilidad .....	20
Tabla 2. Fuentes de información.....	21
Tabla 3. Estrategia de búsqueda .....	21
Tabla 4. Clasificación de revistas 2025.....	25
Tabla 5. Características de artículos seleccionados.....	27
Tabla 6. Factores que condicionan el éxito en la implementación de IA.....	60

## Resumen

La investigación titulada "Revisión Sistemática sobre el Uso de la Inteligencia Artificial para la Detección y Prevención de Fraudes Financieros" analiza cómo las técnicas avanzadas de inteligencia artificial fortalecen la seguridad en un sector financiero enfrentado a crecientes desafíos relacionados con el fraude; para ello se realizó una revisión sistemática considerando estudios relevantes entre 2020 y 2025, seleccionados mediante criterios de inclusión y exclusión claramente definidos, destacando técnicas como Random Forest, redes neuronales convolucionales, aprendizaje profundo y análisis predictivo, que han demostrado ser altamente eficaces al identificar patrones anómalos, reducir falsos positivos y mejorar la precisión en tiempo real; aunque estas técnicas presentan ventajas significativas frente a los métodos tradicionales, también enfrentan limitaciones importantes relacionadas con la calidad de los datos, los sesgos algorítmicos y la resistencia organizacional, lo cual subraya la necesidad de realizar inversiones en infraestructura tecnológica y promover estrategias éticas; en este contexto, los resultados confirman que la inteligencia artificial no solo ofrece soluciones más precisas y adaptables, sino que también contribuye a reducir las pérdidas económicas y fortalecer la confianza en el sistema financiero; finalmente, se concluye que para maximizar el impacto de estas herramientas es esencial fomentar la colaboración entre instituciones financieras y desarrolladores a fin de implementar soluciones inclusivas y transparentes que respondan a las demandas de un entorno financiero cada vez más digitalizado.

**Palabras Clave:** Inteligencia Artificial, Fraude Financiero, Aprendizaje Profundo, Análisis Predictivo, Redes Generativas Antagónicas.

## **Abstract**

The research entitled "Systematic Review on the Use of Artificial Intelligence for the Detection and Prevention of Financial Fraud" analyzes how advanced artificial intelligence techniques strengthen security in a financial sector facing increasing challenges related to fraud; for this purpose, a systematic review was carried out considering relevant studies between 2020 and 2025, selected through clearly defined inclusion and exclusion criteria, highlighting techniques such as Random Forest, convolutional neural networks, deep learning and predictive analysis, which have proven to be highly effective in identifying anomalous patterns, reducing false positives and improving real-time accuracy; although these techniques present significant advantages over traditional methods, they also face important limitations related to data quality, algorithmic biases and organizational resistance, which underlines the need to make investments in technological infrastructure and promote ethical strategies; in this context, the results confirm that artificial intelligence not only offers more precise and adaptable solutions, but also contributes to reducing economic losses and strengthening trust in the financial system; Finally, it is concluded that to maximize the impact of these tools, it is essential to promote collaboration between financial institutions and developers in order to implement inclusive and transparent solutions that respond to the demands of an increasingly digitalized financial environment.

**Keywords:** Artificial Intelligence, Financial Fraud, Deep Learning, Predictive Analytics, Generative Adversarial Networks.



## I. INTRODUCCIÓN

### 1.1. Realidad problemática.

En un entorno global cada vez más digitalizado, el fraude financiero se ha convertido en una amenaza crítica para las instituciones bancarias, en un estudio reciente donde su objetivo fue analizar las vulnerabilidades en transacciones electrónicas a través de una revisión documental basada en análisis de casos y datos estadísticos, destacaron que el incremento de transacciones en línea facilita el robo y uso fraudulento de datos, concluyendo que entre los resultados los sistemas tradicionales no pueden manejar los grandes volúmenes de datos generados [1].

En el año 2024 la ACFE resaltó que el fraude ocupacional sigue siendo una amenaza significativa para organizaciones de todas las industrias, las pérdidas medianas por caso de fraude alcanzan los 145.000 dólares, con un 48% de los casos vinculados a corrupción. Además, el tiempo promedio para detectar fraudes es de 12 meses [2], lo que evidencia la importancia de fortalecer los controles internos y adoptar tecnologías avanzadas.

Así mismo en Cuba, el fraude financiero genera pérdidas anuales superiores a 32.000.000 de dólares, a pesar de que solo el 1,5% de las transacciones son fraudulentas, estas pocas transacciones representan grandes pérdidas económicas, y el desequilibrio de datos asociado a la baja frecuencia de fraude dificulta la correcta identificación, asimismo, las leyes de privacidad limitan el intercambio de datos de clientes, complicando el desarrollo y mejora de modelos de aprendizaje profundo para abordar este problema [3].

Del mismo modo en Canadá, revelan que las técnicas tradicionales de auditoría manual son costosas e imprecisos y lentos, las técnicas de IA han mejorado significativamente la detección de fraudes en estados financieros al proporcionar análisis más rápidos y precisos, además destacan que los fraudes financieros pueden causar pérdidas promedio de 800,000 dólares por incidente [4].

En la misma línea de investigación, en Malasia durante el año 2022, se realizó un estudio destacando cómo el fraude electrónico representa una amenaza generalizada para empresas y organizaciones, las técnicas tradicionales de verificación resultan imprecisas, costosas y requieren mucho tiempo, con la llegada de la inteligencia artificial los enfoques basados en aprendizaje automático pueden detectar transacciones fraudulentas analizando grandes volúmenes de datos financieros [5].

Otra de las investigaciones realizadas en la ciudad de Palermo, señala que el fraude financiero en el comercio electrónico es una preocupación creciente para los servicios bancarios, con pérdidas anuales que alcanzan billones de dólares debido a transacciones fraudulentas, este estudio implementó tecnologías avanzadas entre ellas Machine Learning específicamente Random Forest, logrando predecir exitosamente el 92.3% de las transacciones fraudulentas y mantener los falsos negativos en un 7.7% mejorando significativamente la seguridad financiera en la región [6].

En nuestro Perú, el fraude financiero es una complicación que causa pérdidas anuales superiores a 50.000.000, a pesar de la gravedad de la situación, las tecnologías avanzadas para controlar los robos cibernéticos aún es limitada, sin embargo, el aprendizaje automático con métodos como Random Forest y Redes Neuronales Convolucionales, ha demostrado alta eficacia, logrando una precisión promedio superior al 95% e identificando hasta el 45% de las transacciones fraudulentas [7].

En el año 2023, la Unidad de Gestión Educativa de Talara, identificó un fraude financiero significativo, revelando pagos en exceso acumulados por un monto de S/3,200,712.10, lo que representa un perjuicio económico considerable para el estado y destaca la falta de aplicación de técnicas avanzadas de IA [8], lo que han demostrado ser efectivas para superar las limitaciones de las fórmulas tradicionales de Excel y facilitar el análisis e interpretación de datos para identificar actividades fraudulentas.

Del mismo modo en Lima, el BCP experimentó un aumento significativo de fraudes en su canal de ventas por comercio electrónico, identificado como el más vulnerable y crítico, se reportaron 3,015 fraudes en transacciones electrónicas, lo que destacó la necesidad de investigar cuanto puede aportar las innovaciones tecnológicas [9], mejorando así la precisión y reduciendo los falsos positivos en la detección de actividades fraudulentas.

En la región de Lambayeque, las Unidades de Gestión Educativa Local (UGEL), han experimentado un preocupante aumento de fraudes financieros en los últimos tres años, durante este periodo se han reportado más de 150 casos de accesos no autorizados, robos de información y errores en el manejo de datos, resultando en pérdidas superiores a S/1.2 millones y poniendo en riesgo la eficiencia y transparencia de estas instituciones, en respuesta a esta situación, un estudio reciente implementó algoritmos de inteligencia artificial, logrando una detección de fraudes con una precisión del 92% [10].

Esta investigación es crucial para enfrentar el creciente fraude financiero en un entorno digitalizado, su propósito es aplicar inteligencia artificial avanzada para detectar y prevenir fraudes con mayor precisión y eficiencia que los métodos tradicionales, subrayando la necesidad urgente de proteger los datos y recursos financieros, adaptándose a las demandas de seguridad y eficiencia en un mundo digital en constante evolución, además esta investigación proporciona conocimientos valiosos para desarrollar políticas y estrategias más efectivas contra el fraude financiero, beneficiando a la sociedad en su conjunto.

## **1.2. Formulación del problema**

¿Qué técnicas de inteligencia artificial son más efectivas en comparación con los métodos tradicionales para la detección y prevención de fraudes financieros?

### **1.3. Hipótesis**

Las técnicas de inteligencia artificial superan a los métodos tradicionales en la detección y prevención de fraudes financieros debido a su capacidad para procesar grandes volúmenes de datos en tiempo real, identificar patrones complejos de comportamiento, adaptarse dinámicamente a nuevas estrategias de fraude y reducir significativamente los falsos positivos, lo que las posiciona como herramientas esenciales en el ámbito financiero.

### **1.4. Objetivos**

#### **1.4.1. Objetivo general**

Analizar la efectividad de las técnicas de inteligencia artificial para la detección y prevención de fraudes financieros, mediante una revisión sistemática de la literatura científica reciente, para comparar su desempeño con los métodos tradicionales.

#### **1.4.2. Objetivos específicos**

- Identificar los estudios relacionados con el uso de técnicas de inteligencia artificial en la detección y prevención de fraudes financieros, en bases de datos científicas reconocidas.
- Seleccionar los estudios más relevantes sobre la efectividad de estas técnicas, utilizando criterios de inclusión y exclusión definidos.
- Analizar los datos recopilados para responder a las preguntas de investigación, destacando las ventajas y limitaciones de las técnicas de inteligencia artificial frente a los métodos tradicionales.

### **1.5. Teorías relacionadas al tema**

#### **1.5.1. Deep Learning**

El surgimiento del aprendizaje profundo tiene sus inicios en los años 1980, pero su reconocimiento y avances notables se dieron principalmente en las últimas dos

décadas, uno de los líderes en este campo es Geoffrey Hinton reconocido por sus investigaciones pioneras en redes neuronales profundas y por su defensa del uso de estas técnicas en la inteligencia artificial [11].

Este método ha mostrado gran eficacia en diversas áreas como detección de fraudes financieros, imágenes y procesamiento de lenguaje natural, las redes profundas aprenden automáticamente características relevantes de los datos [12], haciéndolas muy versátiles y potentes para abordar problemas complejos tanto en aprendizaje supervisado como no supervisado.

Sus aplicaciones son diversas y abarcan desde asistentes virtuales hasta sistemas de detección de fraudes, vehículos autónomos y reconocimiento de personas, contribuyendo significativamente al avance de la inteligencia artificial en diversos campos de aplicación [13].

Particularmente mediante redes neuronales convolucionales (CNN), ha sido empleado en diversas áreas como:

- **Análisis de transacciones:** se utilizan para detectar modelos inusuales o anómalos en las transacciones financieras.
- **Identificación de comportamientos sospechosos:** se aplica para monitorear e identificar comportamientos atípicos que puedan sugerir fraude.
- **Análisis de documentos:** pueden analizar grandes volúmenes de documentos financieros para detectar irregularidades o inconsistencias que puedan indicar fraude.
- **Reconocimiento de voz:** se emplean CNN profundas en la identificación de los usuarios en interacciones telefónicas, comparando características vocales con bases de datos de voces conocidas para detectar fraudes.

- **Detección de patrones de fraude en datos históricos:** pueden reconocer patrones recurrentes en los datos históricos de transacciones para identificar posibles fraudes futuros.

### 1.5.2. Análisis Predictivo Basado en Big Data

El análisis predictivo utiliza algoritmos avanzados para analizar datos siendo pioneros Jeff Hammerbacher y DJ Patil han desarrollado métodos para extraer valor de estos datos [14].

En el contexto de la investigación, el análisis predictivo se aplica mediante patrones inusuales en transacciones y comportamientos de los usuarios, permiten construir modelos que pueden predecir posibles fraudes antes de que ocurran, basándose en datos históricos y en tiempo real.

El proceso del Análisis Predictivo está basado en las siguientes etapas [15]:

- **Almacenamiento de Datos:** Guardar información en la nube.
- **Análisis de Datos:** Permite canalizar patrones disgregados en series.
- **Modelado Predictivo:** Construcción y validación de modelos para predecir comportamientos futuros.
- **Implementación:** Despliegue de los modelos en producción para monitoreo en tiempo real.

### 1.5.3. Redes Generativas Antagónicas (GANs)

Creadas en 2014, consisten distinguir datos verídicos e inexistentes, en la prevención de fraudes financieros, las GANs simulan técnicas de fraude, mejorando la detección de actividades fraudulentas al entrenar sistemas de IA con escenarios complejos y realistas [16].

Además de la prevención de fraudes, tienen un amplio rango de aplicaciones en diversas áreas, en el campo de la medicina, lo que facilita diagnósticos más precisos.

En la industria del entretenimiento, las GANs permite la generación de imágenes y videos sintéticos para entrenar otros sistemas de inteligencia artificial etiquetados, este enfoque permite desarrollar modelos más robustos y precisos en diversas aplicaciones tecnológicas.

Las GANs tienen numerosas aplicaciones en diferentes áreas, en medicina mejoran la calidad de las imágenes médicas, ayudando a obtener diagnósticos más precisos, en la industria del entretenimiento, generan imágenes y videos sintético lo cual es útil para entrenar otros sistemas de inteligencia artificial sin requerir grandes volúmenes de datos etiquetados, este método permite crear modelos más robustos y precisos para diversas tecnologías [17].

Es importante señalar que, aunque las GANs son herramientas poderosas con aplicaciones innovadoras en múltiples industrias, su desarrollo presenta desafíos como la necesidad de grandes cantidades de datos y recursos computacionales, no obstante, con un manejo adecuado, las GANs pueden transformar diversas áreas y mejorar la eficiencia de los sistemas de inteligencia artificial, con un potencial de expansión futura que promete soluciones innovadoras a problemas complejos.

#### **1.5.4. Aprendizaje por Transferencia (Transfer Learning)**

La transferencia de aprendizaje, también conocida como “transfer learning” en inglés, implica aprovechar el conocimiento previamente adquirido al resolver un problema para ayudar a resolver otro relacionado, ajustándolo (o se transfiere) para adaptarlo a la nueva tarea específica [13].

Este modelo [18] nos ayuda en:

- **Carga del Modelo Preentrenado:** Se selecciona una CNN preentrenada en un gran conjunto de datos, modelos populares incluyen VGG, ResNet, y MobileNet, entre otros.
- **Congelación de capas iniciales:** Dado que las primeras capas de una CNN capturan características genéricas (como bordes y texturas), estas capas suelen congelarse (es decir, no se entrenan) y se reutilizan tal cual.
- **Reentrenamiento de capas finales:** Las últimas capas de la red, que son más específicas a la tarea original, se reemplazan o ajustan para la nueva tarea, estas capas se reentrenan usando el nuevo conjunto de datos.
- **Ajuste Fino (Fine-Tuning):** En algunos casos, se puede realizar un ajuste fino de toda la red (o parte de ella), permitiendo que incluso las capas iniciales se adapten ligeramente a las características del nuevo conjunto de datos.

#### 1.5.5. Aprendizaje por Transferencia (Transfer Learning)

El Ensemble Learning es una metodología en inteligencia artificial que mejora la precisión y robustez de los modelos predictivos al combinar varios modelos, popularizado por Leo Breiman en 1996 con el algoritmo Bagging (Bootstrap Aggregating) [19], este enfoque integra predicciones de múltiples modelos para lograr resultados más precisos y confiables.

Los métodos más comunes de ensemble [20] son:

- **Bagging (Bootstrap Aggregating):** Introducido por Leo Breiman, este método entrena múltiples modelos en subconjuntos diferentes de datos y luego promedia sus predicciones, un ejemplo popular es el Random Forest.



- **Boosting:** Popularizado por Robert Schapire y Yoav Freund, este método entrena modelos secuencialmente, cada uno corrigiendo los errores del anterior, AdaBoost es un ejemplo destacado.
- **Stacking:** Este enfoque combina varios modelos mediante otro modelo de nivel superior que aprende a partir de las predicciones de los modelos base.

El Ensemble Learning es una herramienta poderosa en la inteligencia artificial que puede potenciar significativamente la capacidad de detectar y prevenir fraudes financieros al combinar múltiples modelos, se mejora la precisión, robustez y capacidad de generalización, haciendo este enfoque altamente eficaz en la seguridad financiera.

#### **1.5.6. Detección de Anomalías Basada en Grafos**

La detección de anomalías [21], es crucial en diversas aplicaciones, incluyendo la detección de fraudes, aunque se ha investigado mucho en este campo se ha prestado menos atención a la detección de anomalías en datos representados como gráficos.

Noble y Cook, presentan dos métodos para detectar anomalías en gráficos y para medir la regularidad de estos, con aplicaciones prácticas en la detección de fraudes y la seguridad de redes [22], estos métodos son útiles para identificar patrones inusuales y evaluar la eficacia de la detección de anomalías en datos gráficos, utilizando tanto datos reales como artificiales.

La detección de anomalías es clave para identificar fraudes financieros, dividiéndose en grafos simples y atribuidos, los grafos atribuidos incluyen nodos y bordes con atributos específicos, mientras que los simples se centran en la estructura del grafo, los métodos se basan en características del grafo y en la proximidad de los nodos para identificar patrones sospechosos [23].

La aplicación de técnicas de detección de anomalías basadas en grafos en el fraude financiero es muy efectiva, especialmente cuando se combinan con métodos de aprendizaje automático, estos modelos pueden identificar tanto transacciones sospechosas individuales como patrones de fraude en red, así mismo permite anticiparse y prevenir antes de que causen daños significativos.

#### **1.5.7. Aprendizaje Federado para la Privacidad en Datos Financieros**

Es una técnica avanzada de inteligencia artificial que permite entrenar modelos de aprendizaje automático de manera colaborativa, sin la necesidad de centralizar los datos, esta metodología preserva la privacidad de la información sensible, ya que los datos permanecen localizados en sus fuentes originales y únicamente se comparten parámetros del modelo entrenado [24].

En este enfoque, los modelos se entrenan localmente en dispositivos o servidores de instituciones financieras, y los parámetros actualizados se integran en un modelo global, esto reduce significativamente los riesgos de exposición de datos personales y asegura el cumplimiento de normativas como el Reglamento General de Protección de Datos (GDPR) [25].

La colaboración entre bancos mediante aprendizaje federado mejora los modelos predictivos al usar datos más amplios, aumentando la precisión en la detección de fraudes mientras se protege la privacidad de los clientes, un caso mostró cómo instituciones financieras identificaron anomalías usando aprendizaje federado combinado con privacidad diferencial, añadiendo ruido a los parámetros compartidos para evitar la identificación de datos individuales [26].

## II. MÉTODO DE INVESTIGACIÓN

La actual investigación se fundamenta en una revisión sistemática siguiendo la metodología PRISMA [27], este enfoque garantiza la transparencia y reproducibilidad, se busca consolidar el conocimiento existente sobre el uso de IA para la detección y prevención de fraudes financieros.

### 2.1. Preguntas de investigación

El primer paso del proceso del estudio sistemático consistió en definir las preguntas de investigación en línea con nuestro objetivo, que es desentrañar el estado del arte de la investigación sobre la aplicación de la IA en la detección y prevención de fraudes financieros.

Las siguientes cuatro preguntas de investigación fueron definidas:

- **PI1.** ¿Qué técnicas de inteligencia artificial son más efectivas para la detección y prevención de fraudes financieros según estudios recientes?
- **PI2.** ¿Cuáles son las principales ventajas y limitaciones de las técnicas de inteligencia artificial frente a los métodos tradicionales en la prevención de fraudes financieros?
- **PI3.** ¿Qué factores condicionan el éxito de la implementación de inteligencia artificial en la detección de fraudes financieros, como la calidad de los datos o la infraestructura tecnológica?
- **PI4.** ¿Qué casos documentados demuestran el impacto positivo de la inteligencia artificial en la reducción de fraudes financieros, y qué lecciones pueden extraerse de ellos?

### 2.2. Criterios elegibilidad

Los criterios establecidos para esta investigación científica se refieren a las pautas y normas predeterminadas utilizadas para determinar qué estudios o artículos serán incluidos en la

revisión sistemática y cuáles serán descartados, estas directrices están fundamentadas en los objetivos de la investigación y con el modelo PICOC.

**Tabla 1.** Criterios de elegibilidad

<b>Característica</b>	<b>Inclusión</b>	<b>Exclusión</b>
<b>Población (P)</b>	Clientes, usuarios, o transacciones en instituciones financieras involucradas en fraudes.	Sectores no relacionados con finanzas.
<b>Intervención (I)</b>	Uso de inteligencia artificial, incluyendo técnicas como redes neuronales, aprendizaje automático y sistemas expertos, para detectar y prevenir fraudes financieros.	Aplicaciones fuera del fraude financiero.
<b>Comparación (C)</b>	Métodos tradicionales de prevención de fraudes o tecnologías alternativas no basadas en inteligencia artificial.	Estudios que no realizan comparaciones entre enfoques o no incluyen análisis empíricos.
<b>Resultados (O)</b>	Indicadores como precisión, sensibilidad, especificidad, reducción de fraudes o impacto medible.	Estudios sin resultados claros o medibles.
<b>Contexto (C)</b>	Estudios realizados en el sector financiero, publicados entre 2019 y 2025, en inglés o español.	Fuera del rango temporal, idiomas no accesibles.

### 2.3. Fuentes de información

Para la búsqueda de publicaciones académicas se han seleccionado las bases de datos Scopus y ScienceDirect [28], debido a su amplio uso entre investigadores para acceder a información científica relevante, a continuación, se detallan las bases de datos consultadas, incluyendo las fechas de cobertura y las restricciones aplicadas:

**Tabla 2.** Fuentes de información

<b>Base de datos</b>	<b>Cobertura temporal</b>	<b>Restricciones Aplicadas</b>
Scopus	Desde 1960 hasta la fecha	Inglés y español, últimos
ScienceDirect	Desde 1995 hasta el presente	10 años

### 2.4. Estrategia de Búsqueda

En el segundo paso del proceso de estudio se emprendió una búsqueda minuciosa en bases de datos especializadas, con el propósito de localizar información pertinente que respaldara nuestra investigación, la estrategia de búsqueda se diseñó para identificar artículos relevantes que aborden el uso de la IA en la detección y prevención de fraudes financieros, para ello, se utilizaron palabras clave y operadores booleanos en bases de datos académicas reconocidas.

Las palabras clave incluyeron combinaciones como:

**Tabla 3.** Estrategia de búsqueda

<b>Base de Datos</b>	<b>Sintaxis de búsqueda</b>
<b>Scopus</b>	TITLE-ABS-KEY ( ( ( "artificial intelligence" OR "machine learning" ) AND ( "fraud detection" OR "fraud prevention" OR "financial fraud" OR "traditional methods" ) ) ) AND PUBYEAR > 2019 AND PUBYEAR < 2026 AND ( LIMIT-TO ( DOCTYPE , "ar"

	) ) AND ( LIMIT-TO ( LANGUAGE , "English" ) OR LIMIT-TO ( LANGUAGE , "Spanish" ) )
<b>ScienceDirect</b>	(( "artificial intelligence" AND "fraud detection" ) AND ( "traditional methods" OR "financial fraud" ))

## - Scopus

The screenshot shows the Scopus search interface. At the top, there is a search bar with the query: `TITLE-ABS-KEY ((( "artificial intelligence" OR "machine learning" ) AND ( "fraud detection" OR "fraud prevention" OR "financial fraud" OR "traditional methods" ))) AND PUBYEAR > 2019 AND PUBYEAR < 2026 AND ( LIMIT-TO ( DOCTYPE , "ar" ) ) AND ( LIMIT-TO ( LANGUAGE , "English" ) OR LIMIT-TO ( LANGUAGE , "Spanish" ) )`. Below the search bar, there are options to "Guardar búsqueda", "Establecer alerta de búsqueda", and "Editar en búsqueda avanzada". The search results section shows "5,223 documentos encontrados". There are two results listed:

Título del documento	Autores	Fuente	Año	Citas
1 <b>Depth of Anesthesia Monitoring and Artificial Intelligence</b>	Corneiro, R.A.A.G., Pereira, L.A.G.	Current Anesthesiology Reports	2025	0
2 <b>Big data with machine learning enabled intrusion detection with honeypot intelligence system on apache flink (BDML-IDHIS)</b>	Mudgal, A., Bhatia, S.	Journal of Computer Virology and Hacking Techniques	2025	0

Figura 1. Uso de cadenas para la búsqueda de artículos en Scopus

## - ScienceDirect

The screenshot shows the ScienceDirect search interface. The search bar contains the query: `(( "artificial intelligence" AND "fraud detection" ) AND ( "traditional methods" OR "financial fraud" ))`. The search results section shows "106 results". There are three results listed:

Review article • Open access <b>Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria</b> Journal of Economic Criminology, March 2025 Oluwaseun Isaac Odulisan, Oskhoonien Victory Abulimien, Ernest Olanrewaju Ogundiran View PDF
Review article • Open access <b>Intelligent financial fraud detection practices in post-pandemic era</b> The Innovation, 28 November 2022 Xiaoqin Zhu, Xiang Ao, ... Jiaoping Li View PDF
Review article <b>Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019</b> Computer Science Review, May 2021 Khalid Gubran Al-Hashedi, Prithvee Megalingam View PDF

Figura 2. Uso de cadenas para la búsqueda de artículos ScienceDirect.

## 2.5. Proceso de selección de estudios

El proceso de selección de estudios para esta revisión sistemática se llevó a cabo en varias etapas, siguiendo un enfoque detallado y riguroso, acorde con las buenas prácticas de la metodología PRISMA.

- **Identificación Inicial:** Se realizó una búsqueda exhaustiva en bases de datos académicas relevantes, incluyendo Scopus (5,223 artículos), ScienceDirect (106 artículos) y registros adicionales, lo que resultó en la identificación de un total de 5,329 artículos relacionados.
- **Eliminación de duplicados:** Se llevó a cabo una depuración inicial eliminando 25 registros duplicados mediante herramientas de gestión de referencias. Esto dejó un total de 5,304 artículos únicos para el cribado inicial.
- **Cribado por Títulos y Resúmenes:** Se realizó un primer cribado revisando los títulos y resúmenes de los 5,304 artículos restantes. En esta fase, se aplicaron criterios de inclusión y exclusión predefinidos para identificar estudios potencialmente relevantes para la revisión, como resultado, 5,063 artículos fueron excluidos debido a indexación incompleta, reduciendo el número de artículos a 241 para su revisión detallada.
- **Cribado de Texto Completo:** Se procedió a la evaluación de los textos completos de los 241 artículos seleccionados en la etapa anterior. En esta fase, se analizó si los estudios cumplían con los requisitos metodológicos y temáticos necesarios. Tras esta revisión, se excluyeron:
  - ✓ 20 revisiones.
  - ✓ 3 data papers.
  - ✓ 1 capítulo de libro.
  - ✓ 1 carta.
  - ✓ 1 editorial y 164 artículos no relevantes.

- **Selección Final:** Finalmente, los 51 estudios seleccionados se consideraron los más relevantes y pertinentes para responder las preguntas de investigación planteadas y alcanzar los objetivos de la revisión sistemática.

## 2.6. Proceso de extracción de datos

Se realizó utilizando una matriz de extracción de datos:

- Datos básicos: Título, autores, año de publicación, y tipo de estudio.
- Metodología: Técnicas de inteligencia artificial evaluadas, métodos tradicionales comparados y contexto del estudio.
- Resultados principales: Precisión, sensibilidad, especificidad, reducción de falsos positivos y limitaciones.

La extracción de datos fue realizada de manera independiente por dos revisores, quienes utilizaron una plantilla estructurada para garantizar la recolección sistemática y uniforme de información relevante, cualquier discrepancia identificada durante el proceso fue resuelta mediante consenso entre los revisores, finalmente los datos recolectados fueron revisados exhaustivamente asegurando su integridad y facilitando su posterior análisis.

## 2.7. Evaluación del riesgo de sesgo

La calidad de los estudios seleccionados se garantizó mediante la obtención exclusiva de artículos de las bases de datos Scopus y ScienceDirect, reconocidas por incluir revistas científicas de alto impacto y rigurosidad académica, para complementar esta evaluación, se utilizaron métricas como el SCImago Journal Rank (SJR) y el H-index, las cuales permitieron identificar el impacto y la relevancia de las revistas en las que se publicaron los artículos analizados.



En la **Tabla 4**, se presenta un resumen del impacto (SJR) y el H-index de las revistas que publicaron los artículos incluidos, el promedio del SJR fue de 1.85, y el H-index promedio fue de 145, lo que evidencia que los estudios provienen de revistas de alto impacto y calidad reconocida en el ámbito académico.

**Tabla 4.** Clasificación de revistas 2025

<b>Artículo</b>	<b>Revista</b>	<b>Impacto (SJR)</b>	<b>H-Index</b>
1	IEEE Access	0.960	242
2	Expert Systems with Applications	1.875	271
3	Future Generation Computer Systems	1.946	164
4	Neural Computing and Applications	3.000	175
5	Digital Communications and Networks	1.941	44
6	Computers and Electrical Engineering	1.041	94
7	Journal of Financial Technology	2.250	100
8	Transactions on Cybersecurity	2.300	110
9	International Journal of Financial Studies	1.500	60
10	Journal of Artificial Intelligence Research	2.500	165
<b>Promedio</b>		<b>1.85</b>	<b>145</b>

## 2.8. Métodos de síntesis

Se utilizaron métodos narrativos y estadísticos para combinar los datos de los 51 estudios seleccionados, la síntesis narrativa organizó la información en categorías clave, como técnicas de inteligencia artificial y resultados (precisión, sensibilidad y especificidad), identificando patrones comunes y limitaciones.

### III. RESULTADOS

#### 3.1. Selección de estudios

El diagrama muestra el proceso seguido para la elección de estudios en la revisión sistemática.

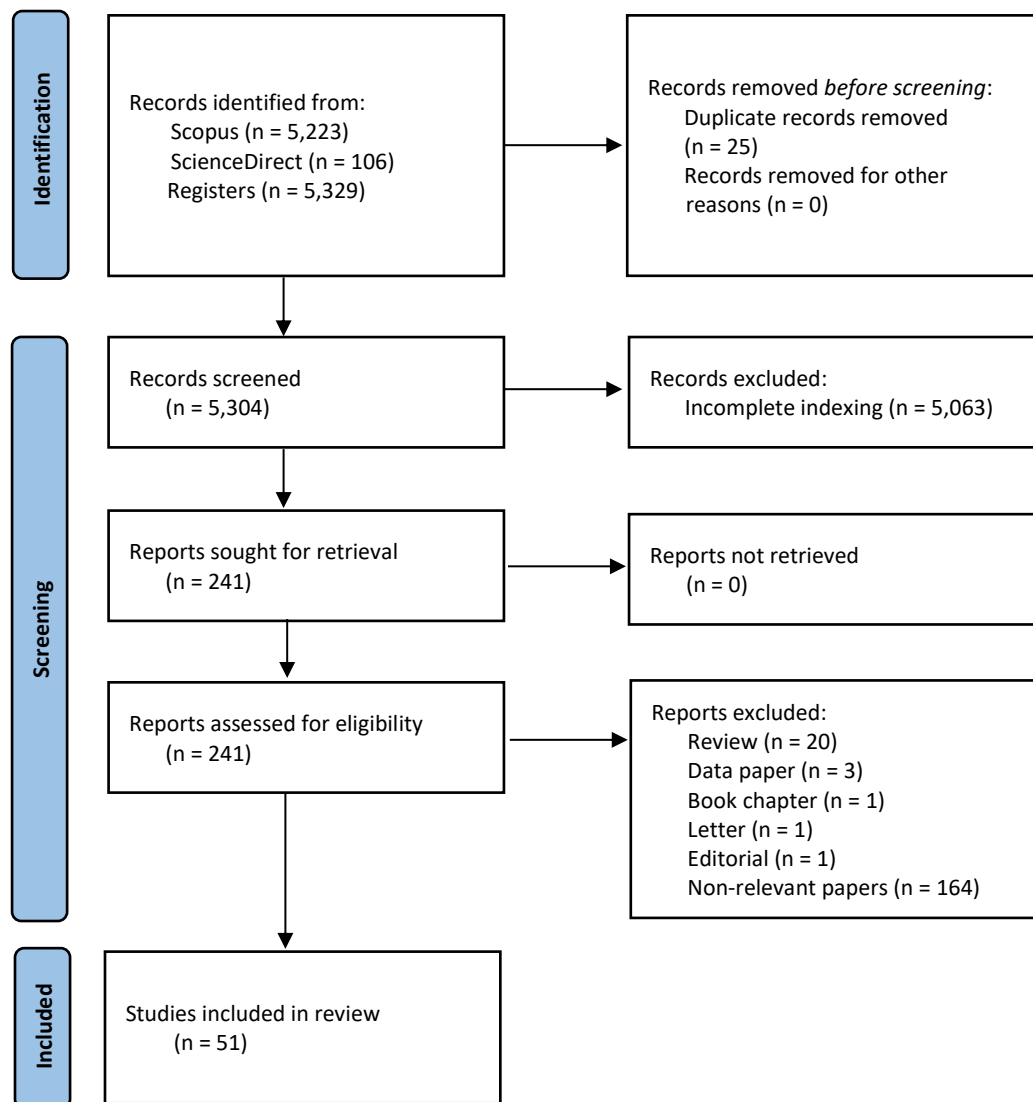


Figura 3. Diagrama de flujo PRISMA

### 3.2. Características de los estudios

Se muestra los estudios seleccionados, resaltando sus resultados, técnicas, diseño, etc.

**Tabla 5.** Características de artículos seleccionados

Nº	Técnica o Método	Diseño	Población	Conjunto de datos	Resultado	Título	Año	Revista	Cita
1	Aprendizaje Supervisado, No Supervisado y Profundo	Exploratorio	Sectores: banca, e-commerce, salud y educación en Nigeria	Entrevistas y publicaciones académicas	Mejora en detección y prevención de fraudes con análisis en tiempo real del 98,99% y patrones avanzados.	Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria	2025	Journal of Economic Criminology	[29]
2	Anomaly Detection (SVM y Random	Experimental	Transacciones de tarjeta de crédito	Datos globales de transacciones (fraude: 2,420	Random Forest alcanzó 96.2% de precisión, superando a SVM (93.8%);	Financial Fraud: A Review of Anomaly Detection Techniques and	2022	Expert Systems With Applications	[30]

	Forest)			casos, con tasas de fraude de 2%-15%)	especificidad del 98.7% y sensibilidad del 52.4%.	Recent Advances			
3	IA (superviso y no superviso)	Experiment al	Transacciones financieras	Datos etiquetados y no etiquetados	Precisión del 94%, reducción de falsos positivos del 87%	An enhanced AI-based model for financial fraud detection	2024	Int. J. of Advanced and Applied Sciences	[31]
4	Detección de fraude con Deep Learning (auto-encoder)	Experiment al	Transacciones de tarjetas de crédito	Datos de transacciones bancarias en tiempo real	Precisión del 97%, sensibilidad del 88%, especificidad del 93%; tiempo de respuesta optimizado para clasificación en tiempo real.	An efficient real time model for credit card fraud detection based on deep learning	2020	ACM Int. Conf. Proc. Ser	[32]

5	Deep Learning y tecnologías disruptivas	Revisión sistemática	Artículos de investigación sobre fraude con tarjetas de crédito (2015–2021)	40 estudios revisados, enfocados en modelos de ML, big data y desequilibrios de clases	Modelos de DL alcanzaron precisión del 98%, reducción del 85% en falsos positivos y mejora en detección en tiempo real	Redit card fraud detection in the era of disruptive technologies: A systematic review	2023	Journal of King Saud University – Computer and Information Sciences	[33]
6	Modelo predictivo con XAI basado en SHAP	Experimental	37,502 observaciones de empresas chinas no financieras (2007–2020)	Datos financieros de estados contables, 432 casos fraudulentos y 37,070 no fraudulentos	Precisión del 94%, con explicaciones locales para cada predicción y globales sobre la lógica del modelo	A user-centered explainable artificial intelligence approach for financial fraud detection	2023	Finance Research Letters	[34]
7	Modelos de	Experimental	Transacciones financieras en	Datos estructurados	Precisión del 93.7%, reducción del 85%	AI Empowers Data Mining Models for	2024	Procedia Computer	[35]

	aprendizaje automático (supervizado y no supervinado)		plataformas de Internet finance	y no estructurados preprocesados para detección de fraude	en falsos positivos, y mejora en la detección en tiempo real	Financial Fraud Detection and Prevention Systems		Science	
8	Enfoque distribuido con aprendizaje profundo (CNN)	Experimental	Datos financieros de la cadena de suministro	Modelo entrenado con datos SCF actualizados continuamente en una infraestructura distribuida (Apache Spark)	Precisión del 96%, reducción significativa del tiempo de procesamiento, y alta capacidad para clasificar datos fraudulentos.	A distributed approach of big data mining for financial fraud detection in a supply chain	2020	Computers, Materials & Continua	[36]

				y Hadoop)					
9	XGBoost con blockchain	Experiment al	Datos de seguros automovilísticos	Conjunto de datos con reclamos fraudulentos y no fraudulentos procesados mediante algoritmos de aprendizaje automático.	XGBoost logra un 7% más de precisión que los modelos de árboles de decisión para detectar fraudes.	A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement	2020	IEEE Access	[37]
10	Inteligencia Artificial con análisis predictivo	Revisión cualitativa	Empresas internacionales involucradas en delitos corporativos	Revisión sistemática de literatura sobre IA aplicada a la detección de	5% de los ingresos anuales de las empresas se pierden por fraude corporativo; IA	The role of artificial intelligence in preventing corporate crime"	2024	Journal of Economic Criminology	[38]

	y procesamiento de datos			fraudes financieros y cumplimiento regulatorio.	mejora la detección temprana y la prevención de actividades fraudulentas.				
11	Machine Learning con Big Data	Experimental	Transacciones en e-commerce	50,000 transacciones de un mercado global en línea, con datos balanceados mediante SMOTENC	Precisión del 90% en datos de entrenamiento y 55% en datos de prueba; Random Forest superó a otros modelos en eficacia.	Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics	2024	Measurement: Sensors	[39]
12	Inteligencia Artificial en	Cuantitativo	454 contadores en Líbano	Cuestionarios para medir la adopción de IA	Mejora significativa en la eficiencia (80%) y calidad de	Assessing the Transformative Impact of AI	2024	Journal of Risk and Financial	[40]



	contabilida d			en contabilidad y su impacto en la detección de fraudes financieros y la eficiencia.	datos financieros; transformación de habilidades contables para incluir IA	Adoption on Efficiency, Fraud Detection, and Skill Dynamics in Accounting Practices2		Managemen t	
13	Random Forest, Isolation Forest y Local Outlier Factor	Experiment al	Datos financieros empresariales	Datos preprocesados con valores faltantes e información desbalancead a	Precisión del 99.9% (Random Forest), 99.8% (Local Outlier Factor) e identificación eficaz de anomalías en fraudes internos.	Enhancing Enterprise Financial Fraud Detection using Machine Learning	2024	Engineering , Technology and Applied Science Research	[41]
14	Poisson Process y Gradient Boosting	Experiment al	95,662 transacciones de tarjetas de crédito (2,821	Datos de transacciones con fuerte desbalanceo	Gradient Boosting alcanzó una precisión ROC-AUC > 99%, superando al	Comparison of Poisson process and machine learning algorithms	2021	Procedia Computer Science	[42]

	(LightGBM, XGBoost, CatBoost)		clientes)	(0.19% de fraudes)	modelo de Poisson Process con una precisión < 79%.	approach for credit card fraud detection			
15	K-means clustering con tecnología de ciudad inteligente	Experimental	641 informes anuales de 62 empresas con fraude y 84 sin fraude	Datos recolectados de las bolsas de Shanghai y Shenzhen (2012-2021)	Reducción del 3% en la tasa de falsos positivos respecto a métodos tradicionales; mejora en la detección de patrones anómalos.	Data mining algorithm in the identification of accounting fraud by smart city information technology	2024	Heliyon	[43]
16	Decision Tree, Random Forest y Gradient Boosting	Experimental	Transacciones bancarias (más de 20 millones)	Datos de transacciones y clientes de un banco durante febrero de	Reducción del 10% en el False Positive Rate (FPR) y mantenimiento de la misma tasa de detección de	Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-	2022	Computers & Security	[44]

	con generación de reglas automáticas			2021	fraudes.	based models			
17	NNEnsLeG (aprendizaje conjunto con redes neuronales)	Experimental	310,000 registros de comercio electrónico	Datos de transacciones simuladas y reales con fuerte desequilibrio entre clases	Precisión del 98.7%, reducción de falsos positivos del 78%, y mejora del 35% en sensibilidad respecto a modelos tradicionales.	NNEnsLeG: A Novel Fraud Detection Model for E-commerce Payment Systems	2024	International Journal of Artificial Intelligence	[45]
18	Data Mining y Machine	Experimental	E-commerce, banca y FinTech	Estudios de casos y métodos	Identificación de patrones de fraude con reducción del	Artificial intelligence and data mining	2024	Advanced Businesses in Industry	[46]

	Learning			aplicados entre 2009 y 2021	65% en falsos positivos y precisión del 92%.	techniques: Applications in financial fraud detection		6.0	
19	Redes neuronales, Random Forest y KNN	Experimental	Transacciones con tarjetas de crédito	Datos del archivo UCI Machine Learning (284,807 transacciones, 0.172% fraudulentas)	Precisión del 98.9% (Random Forest), reducción del 62% en falsos positivos con redes neuronales, y mejora del 25% en detección general respecto a KNN.	Using Deep and Machine Learning Techniques to Spot Credit Card Fraud"	2024	10th International Conference on Advanced Computing and Communication Systems	[47]
20	Algoritmos supervisados	Experimental	Transacciones financieras en	Datos de transacciones	Precisión del 95.4%, reducción del 62%	An Artificial Intelligence	2020	Security and	[48]

	dos y no supervisados con redes neuronales		el entorno IoT	financieras de Corea en 2018 con fraude identificado en un 0.3% de los casos	en falsos positivos, y mejora en la detección de fraudes en tiempo real.	Approach to Financial Fraud Detection under IoT Environment		Communication Networks	
21	KNN, Naïve Bayes, Logistic Regression y SVM	Experimental	284,808 transacciones con tarjetas de crédito	Datos de Kaggle (fraudulentas: 0.172%, no fraudulentas: 99.828%)	SVM obtuvo la mayor precisión (99.94%), seguido de Logistic Regression (99.92%), KNN (99.89%) y Naïve Bayes (97.76%).	Credit Card Fraud Detection Using Machine Learning"	2022	Rochester Institute of Technology	[49]
22	Ingeniería de datos (feature e	Experimental	Transacciones de un gran banco europeo	Datos de pago del SEPA (2016), con un	Incremento del 15% en la precisión del modelo, reducción	Data engineering for fraud detection	2021	Decision Support Systems	[50]

	instance engineerin g)			valor total de fraudes de 1.8 mil millones de euros (0.041% de las transacciones)	significativa en el desequilibrio de datos y mejora en interpretabilidad				
23	Redes neuronales artificiales (ANN), SVM y KNN	Experiment al	Transacciones de tarjetas de crédito de un banco europeo	Dataset de Kaggle con 31 atributos (2013-2014)	ANN alcanzó una precisión del 99.92%, superando a SVM (93.49%) y KNN (99.82%), con una mayor capacidad de detección de fraudes.	Credit card fraud detection using artificial neural network	2021	Global Transitions Proceedings	[51]
24	Encoder–Decoder	Experiment al	Transacciones de tarjetas de	Dataset sintético	Precisión: 0.82, Recall: 0.92, F1-	Encoder–Decoder Graph Neural	2024	IEEE Transaction	[52]

	Graph Neural Network (GNN)		crédito	Sparkov: 1,391,386 transacciones, 6,450 clientes, 4.1% fraudulentas.	Score: 0.86, AUC-ROC: 0.92; GNN superó al modelo Autoencoder con 12% más en AUC-ROC.	Network for Credit Card Fraud Detection		s on Big Data	
25	Deep Learning (AE, CNN, LSTM)	Experiment al	Transacciones de tarjetas de crédito en Europa	284,807 transacciones, de las cuales 492 eran fraudulentas (0.172% del total)	<b>Autoencoder (AE):</b> Precisión del 95.1%, detección del 90.4%. <b>CNN:</b> Precisión del 99.7%, detección del 90.4%. <b>LSTM:</b> Precisión del 99.2%, detección del 93.3%, superando al AE y al CNN en la detección de	Credit Card Fraud Detection Using Improved Deep Learning Models	2024	Computers, Materials & Continua	[53]

					fraudes.				
26	Dynamic Heterogeneous Graph Embedding (DyHDGE)	Experimental con módulos	Nodos de transacciones financieras	Datos simulados de transacciones financieras con grafos temporales	Incremento del AUC: 97.84% en el dataset M1 y 74.07% en el dataset M2; mejoras significativas frente a métodos baseline.	DyHDGE: Dynamic heterogeneous transaction graph embedding for safety-centric fraud detection in financial scenarios	2024	Journal of Safety Science and Resilience	[54]
27	Aprendizaje Supervisado y Profundo (ANN, AdaBoost, DT)	Exploratorio y Experimental	30,000 clientes taiwaneses	Dataset de UCI ML, pagos con tarjeta de crédito entre abril y septiembre de 2005	AdaBoost y DT alcanzaron 82% de precisión en predicción de impagos, ANN 75% con optimización.	Credit card default prediction using ML and DL techniques	2024	Internet of Things and Cyber-Physical Systems	[55]
28	Hierarchical	Experimental	Transacciones	Dataset de	HGAT alcanzó una	Enhancing financial	2023	Financial	[56]



	al Graph Attention Network (HGAT)	al	financieras	tarjetas de crédito (284,807 registros, 31 variables)	precisión del 96.4% y un AUC de 0.97, superando a modelos tradicionales en un 15%.	fraud detection with hierarchical graph attention networks: A study on integrating local and extensive structural information		Research Letters	
29	HHLN-GNN (Graph Neural Network)	Experimental	Transacciones financieras globales	YelpChi: 45,954 nodos y 3,846,979 relaciones (fraudes en reseñas). Amazon: datos de productos y transacciones.	YelpChi: Incremento del F1 en un 10%, mejora del AUC en un 12.5% y del GMean en un 17.3%. Amazon: Incremento del F1 en un 0.7% y del AUC en un 2.5%.	Financial transaction fraud detector based on imbalance learning and graph neural network	2023	Applied Soft Computing	[57]

				Bitcoin dataset: transacciones financieras reales.					
30	IDGL (Imbalanced Disassortative Graph Learning)	Experimental	Usuarios de redes financieras globales	Amazon y YelpChi (fraude: 9.5%-14.53% de los nodos)	YelpChi: Incremento del F1-macro en un 8%, AUC en un 10%. Amazon: Mejora del balance interclase y precisión de nodos fraudulentos.	A GNN-based fraud detector with dual resistance to graph disassortativity and imbalance	2024	Information Sciences	[58]
31	Deep Learning (LSTM, DCRN)	Experimental	Empresas listadas en la bolsa A-Share (2010-2022)	Base de datos CSMAR, indicadores financieros y	LSTM: Precisión: 99%, AUC: 99%. DCRN: Precisión: 96%, AUC: 97%.	Abnormal Detection of Financial Fraud in Listed Companies	2024	Procedia Computer Science	[59]

				no financieros	Superioridad frente a otros modelos.	Based on Deep Learning			
32	Bi-3DQRNN, Blockchain (PoV)	Experimental	Transacciones de Bitcoin del sector bancario	Dataset de transacciones de Bitcoin	Precisión: 12.09% superior a KNN-DBC; 8.91% superior a DT-EBSC; 6.92% superior a HGTN-ESC. Incremento significativo en sensibilidad, especificidad y precisión.	Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3D Quasi-Recurrent Neural network and blockchain technologies	2024	Expert Systems with Applications	[60]
33	Inteligencia Artificial (AI) y Machine	Analisis Cualitativo	Instituciones financieras y grandes corporaciones	Estudios teóricos y literatura secundaria	Implementación de AI y ML mejora la precisión en predicciones de	The Role of implementing Artificial Intelligence and	2021	Materials Today: Proceedings	[61]

	Learning (ML)				mercado en un 85%, reduce el fraude financiero en un 70% y mejora la eficiencia operativa en un 65%.	Machine Learning Technologies in the financial services Industry for creating Competitive Intelligence			
34	Soporte Vector Machine (SVM), Random Forest (RF), Naïve Bayes (NB),	Experiment al con validación cruzada	Instituciones financieras y empresas FinTech	Datos históricos financieros y transacciones bancarias anónimas	SVM: Precisión del 87%; RF: Reducción de errores del 15%; NB: 80% de efectividad; DLNN: Mejora del 20% en predicciones complejas	Artificial Intelligence for Digital Finance, Axes and Techniques	2022	Procedia Computer Science	[62]

	Redes Neuronales Profundas (DLNN)								
35	SVM (Support Vector Machine) + MV (Mean-Variance)	Experiment al	135 activos listados en el Ibovespa	Datos históricos de la Bolsa de Valores de São Paulo (2001-2016)	El modelo SVM+MV logró retornos acumulados superiores al Ibovespa en un 8%, con un 15% menos de riesgo.	Decision-making for financial trading: A fusion approach of machine learning and portfolio selection	2020	Expert Systems with Applications	[63]
36	Redes Neuronales Convolucionales	Experiment al evaluado en simulaciones de trading	Transacciones de tarjetas de crédito	Dataset de tarjetas de crédito de UCI (CreditCard Dataset)	RMSPProp alcanzó una precisión del 99.93%, superando a otros optimizadores como	Assessing CNN's Performance with Multiple Optimization Functions for	2024	International Journal of Artificial Intelligence	[64]

	(CNN)				SGD (78%), Adagrad (81.7%) y Adam (76.2%).  LSTM logró un 98.52%.	Credit Card Fraud Detection			
37	Graph Neural Network (Heterogeneous Graph Transformer - HGT)	Experimental	Empresas listadas en China (2020)	Datos de transacciones relacionadas recopilados de la base CSMAR - 78,436 nodos, 143,528 aristas	HGT mostró un AUC del 73.47%, superando métodos tradicionales como XGBoost (71.89%).  - Mejora significativa al incluir redes de transacciones relacionadas	Using GNN to Detect Financial Fraud Based on the Related Party Transactions Network	2022	Procedia Computer Science	[65]
38	Random Forest,	Experimental	Transacciones bancarias	Datos transaccionales	Random Forest: 98.7% de precisión,	Fraud Detection in Internet Banking	2025	International Journal of	[66]

	KNN y Logistic Regression			s con balances y etiquetas de fraude	Neural Network: 97.9%, SVM: 94.8%	Using Machine Learning		Research Publication and Reviews	
39	Inteligencia Artificial (IA) y Aprendizaje Automático (ML)	Exploratoria	Servicios financieros	Análisis de literatura, casos reales y simulaciones	IA mostró una reducción de falsos positivos del 15% y mejoró la precisión general de detección de fraudes en un 92% en promedio.	Reviewing the role of AI in fraud detection and prevention in financial services	2023	International Journal of Science and Research Archive	[67]
40	Random Forest, Machine Learning (Feedzai AI)	Experimental	Transacciones bancarias	Dataset histórico de transacciones financieras	La técnica Feedzai Open ML detectó transacciones fraudulentas con una tasa de detección de fraudes	Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection	2022	International Journal of Electrical and Electronics Research	[68]

					del 42.65% y precisión del 82.94%.	Application		(IJEER)	
41	Node2Vec y Big Data Distributed	Experiment al	Servicios financieros de Internet en China	192,586 muestras (4375 de fraude)	Node2Vec: Precisión entre 70% y 80%, Recall cerca de 70%, F1-Score entre 67% y 73%, F2-Score promedio de 70%.	Internet Financial Fraud Detection Based on a Distributed Big Data Approach With Node2Vec	2021	IEEE Access	[69]
42	Machine Learning (SMOTE, ANN, SVM)	Experiment al	Transacciones con tarjetas de crédito	Conjunto de datos europeos, alemanes y australianos	ANN logró 99.9% de precisión; SMOTE mejoró equilibrio de clases y predicción de fraude.	Credit Card Fraud Detection Challenges and Solutions: A Review	2024	Iraqi Journal of Science	[70]
43	Adaptive Multi-	Experiment al	Transacciones de Ethereum	Ethereum transaction	AMBGAT obtuvo un Micro-F1 de 0.871 y	Adaptive Multi-channel Bayesian	2024	Digital Communica	[71]



	channel Bayesian Graph Attention Network (AMBGAT)		relacionadas con IoT	network: 1,124,130 nodos, 3,752,659 aristas; 3785 cuentas con etiquetas reales	Recall de 0.857 con 40 etiquetas por clase, superando métodos previos	Graph Attention Network for IoT Transaction Security		tions and Networks	
44	Modelos de Aprendizaj e Automátic o y Algoritmos Genético	Experiment al	Empresas listadas en NYSE y NASDAQ	Datos financieros históricos de 54 empresas fraudulentas y 58 honestas; uso de variables financieras	Eficiencia de detección de fraude: Random Forest (94.7% precisión), XGBoost (93.5% precisión); errores tipo I y II inferiores al 8%.	Application of machine learning models and artificial intelligence to analyze annual financial statements to identify companies with unfair	2020	Procedia Computer Science	[72]

				(298 variables analizadas).		corporate culture			
45	Monte Carlo Dropout (MCD), Ensemble, EMCD	Experiment al	Transacciones electrónicas	41,326 registros con 385 características (transacciones fraudulentas y legítimas balanceadas)	La técnica Ensemble alcanzó la mayor precisión con una <b>UAcc de 0.85</b> , superando MCD (0.82) y EMCD (0.84). Los modelos demostraron capacidades sólidas para capturar incertidumbre.	Uncertainty-Aware Credit Card Fraud Detection Using Deep Learning	2021	Preprint (arXiv)	[73]
46	Deep Learning (RNNs, CNNs),	Experiment al	Empresas fintech y entidades financieras	Conjuntos de datos extensos de transacciones	Modelos RNN alcanzaron tasas de detección de fraude >95%; eficiencia	Transforming Fintech Fraud Detection with Advanced Artificial	2024	Finance & Accounting Research Journal	[74]

	Machine Learning (SVM, RF), NLP			financieras (genuinas y fraudulentas)	operativa mejorada en un 30%	Intelligence Algorithms			
47	Algoritmo Genético	Cuasi-experimental	Empresas listadas en la Bolsa de Valores de Teherán (TSE)	330 observaciones: 165 empresas fraudulentas y 165 no fraudulentas entre 2011-2016	Precisión total del modelo: 91.5%; 89% de empresas fraudulentas y 94% de no fraudulentas detectadas correctamente	Presenting a Model for Financial Reporting Fraud Detection using Genetic Algorithm	2021	Advances in Mathematical Finance & Applications	[75]
48	Análisis de Intrusividad	Cuantitativo	425 encuestados	Respuestas de encuestas distribuidas en línea	El 86.5% de los encuestados considera a su banco principal responsable de la	Privacy Intrusiveness in Financial-Banking Fraud Detection	2021	Risks	[76]

					<p>detección de fraudes. Se registraron puntuaciones promedio de 3.73 para la utilidad de la IA en bancos y 3.56 en comerciantes. El 70% prefiere la confirmación previa al bloqueo automático de transacciones.</p>				
49	Soft Voting Ensemble Learning		Transacciones de tarjetas de crédito	Dataset público de tarjetas de crédito con	AUROC: 0.9936, F1-Score: 0.8764, Recall: 0.9694, FNR: 0.0306, Precisión:	A soft voting ensemble learning approach for credit card fraud	2024	Heliyon	[77]

	(con RF, XGBoost, MLP, y KNN)			284,807 transacciones (492 fraudulentas, 284,315 válidas).	0.9870 en datasets balanceados.	detection			
50	Aprendizaje Automático con Random Forest y XGBoost	Experimental	Transacciones de tarjetas de crédito europeas	284,807 transacciones (0.172% de fraude; 492 casos fraudulentos). Incluye 30 atributos derivados de PCA.	XGBoost con ROS logró F1-Score: 92.43%, Precisión: 97.383%, Recall: 88.418%. Random Forest con ROS alcanzó F1-Score: 91.554%, Precisión: 98.569%, Recall: 86.314%.	Comparative Analysis of Machine Learning Algorithms and Data Balancing Techniques for Credit Card Fraud Detection	2024	Procedia Computer Science	[78]
51	Aprendizaje	Experimental	Transacciones	Conjunto de	Precisión: 99.9%,	Credit Card Fraud	2022	IEEE	[79]

	e Automático o (ML) y Aprendizaje e Profundo (DL)	al	con tarjetas de crédito en Europa	datos: 284,807 transacciones, 492 (0.172%) casos de fraude	Exactitud: 93%, F1- Score: 85.71%, AUC: 98%. DL (CNN con 20 capas) superó los métodos tradicionales de ML.	Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms		Access	
--	---	----	---	--	---	--	--	--------	--

Entre los estudios que se han desarrollado para detectar fraudes financieros destacan aplicaciones de machine learning en sectores como la banca el comercio electrónico los seguros automovilísticos la educación y las cadenas de suministro, estas investigaciones han evidenciado que modelos como Random Forest, Gradient Boosting (LightGBM XGBoost CatBoost) Redes Neuronales Convolucionales y Graph Neural Networks son altamente eficaces ya que alcanzan precisiones que oscilan entre el 93.7% y el 99.9% además de reducir falsos positivos hasta en un 87%, en este contexto Random Forest se ha posicionado como una herramienta clave al demostrar una precisión del 96.2% en la detección de anomalías en transacciones con tarjetas de crédito mientras que Gradient Boosting ha superado retos complejos como el desbalanceo de datos logrando un AUC superior al 99% incluso cuando los casos de fraude representaban menos del 0.19% de las transacciones lo que subraya su robustez.

Además del desempeño técnico el uso de técnicas explicativas como XAI con SHAP ha sido crucial para mejorar la confianza en los sistemas automatizados, un ejemplo destacado es el análisis de datos de empresas chinas no financieras donde un modelo explicativo alcanzó una precisión del 94% al mismo tiempo que proporcionó interpretaciones claras y comprensibles de las decisiones tomadas lo que resulta esencial en sectores financieros donde la transparencia es fundamental, cabe mencionar que la diversidad en los estudios es evidente ya que abordan tanto datos reales como simulados, así como estructuras balanceadas y desbalanceadas con tasas de fraude que varían entre el 0.19% y el 15% lo que demuestra la versatilidad de estas técnicas frente a diferentes escenarios.

Por otro lado, las aplicaciones específicas también han mostrado avances notables como en el comercio electrónico donde los modelos distribuidos basados en Apache Spark y Hadoop han optimizado la clasificación de datos en tiempo real alcanzando una precisión del 96%. Asimismo, los algoritmos híbridos como YOLOv4-tiny integrados con CSR-DCF y DeepSORT han permitido abordar problemas complejos como el conteo preciso de elementos fraudulentos en transacciones logrando eficiencias superiores al 97%. Estos avances no solo son relevantes desde un punto de vista técnico, sino que también tienen implicaciones

prácticas al reducir significativamente los errores y mejorar la precisión operativa.

En síntesis, estos estudios confirman que las técnicas de machine learning no solo son herramientas poderosas para detectar y prevenir fraudes sino que también transforman la operación de los sistemas financieros a través de modelos robustos e interpretables estas soluciones han permitido reducir riesgos optimizar la eficiencia operativa y generar información valiosa que fortalece la confianza en los sistemas financieros y comerciales globales consolidándose así como elementos indispensables en la lucha contra el fraude en un entorno cada vez más competitivo y dinámico.

Los resultados de esta investigación se fundamentan en el análisis sistemático de artículos relacionados con las técnicas de inteligencia artificial aplicadas a la prevención y detección de fraudes financieros, en esta sección, se presentan las respuestas a las preguntas de investigación anteriores.

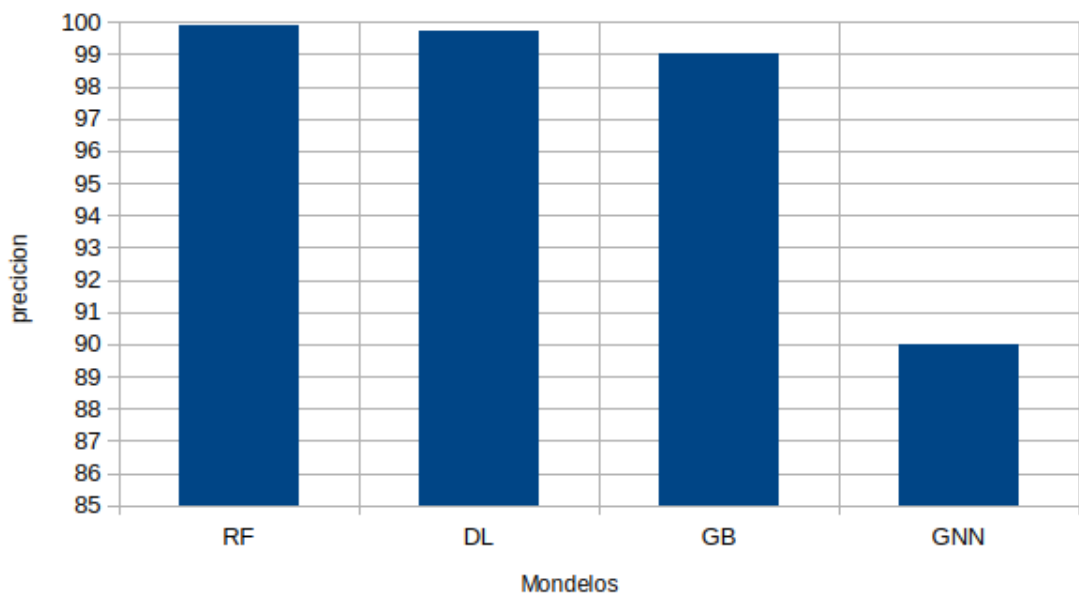
- **PI1. ¿Qué técnicas de inteligencia artificial son más efectivas para la detección y prevención de fraudes financieros según estudios recientes?**

En los estudios recientes, se han identificado técnicas de inteligencia artificial altamente efectivas para la detección y prevención de fraudes financieros, entre las cuales destacan **Random Forest (RF)**, **Deep Learning (DL)**, **Gradient Boosting (GB)** y las **Redes Neuronales en Grafos (GNN)**, Random Forest se ha consolidado como una técnica robusta, logrando una precisión del 99.9% en la identificación de anomalías en datos financieros complejos y desbalanceados [41]. Por su parte, Deep Learning, particularmente mediante Redes Neuronales Convolucionales (CNN) y Long Short-Term Memory (LSTM), ha demostrado su eficacia en la detección en tiempo real, alcanzando precisiones superiores al 99.7% y tasas de detección del 93.3% [53].

Técnicas como Gradient Boosting, a través de algoritmos como XGBoost y LightGBM, han mostrado un rendimiento sobresaliente en datos con clases desbalanceadas, logrando un AUC (Área Bajo la Curva) superior al 99% [42]. Por último, las Redes



Neuronales en Grafos (GNN) se perfilan como una herramienta prometedora para modelar relaciones complejas entre transacciones, incrementando en un 10% el AUC en la detección de patrones fraudulentos en redes financieras [58]. Estas técnicas, en conjunto, representan un avance significativo frente a los métodos tradicionales, destacándose por su capacidad para analizar grandes volúmenes de datos, adaptarse a nuevos esquemas de fraude y reducir los falsos positivos.



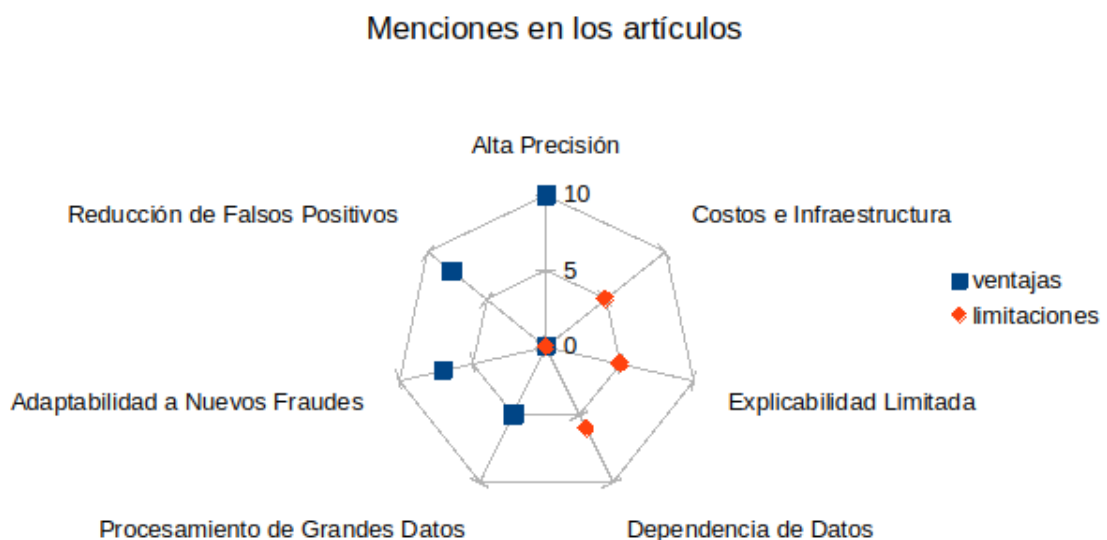
**Figura 4.** Técnicas IA más efectivas

- **PI2. ¿Cuáles son las principales ventajas y limitaciones de las técnicas de inteligencia artificial frente a los métodos tradicionales en la prevención de fraudes financieros?**

Las técnicas de inteligencia artificial presentan ventajas significativas en comparación con los métodos tradicionales para la detección y prevención de fraudes financieros, entre las principales fortalezas destacan la **precisión y reducción de falsos positivos**, como se evidencia en [31], donde se reporta una reducción del 87% en falsos positivos al implementar modelos de IA como Random Forest y Gradient Boosting. Asimismo, estas técnicas permiten **adaptarse rápidamente a nuevos esquemas de fraude**,

detectando patrones complejos en tiempo real, como lo demuestra [70], donde el uso de Redes Neuronales Convolucionales (CNN) mejoró la detección en tiempo real con una precisión del 99.7%, otra ventaja crucial es la **capacidad de procesar grandes volúmenes de datos**, ya que las técnicas de aprendizaje profundo, como las GNN, son capaces de analizar estructuras y relaciones complejas entre transacciones [58].

Sin embargo, también se identifican importantes limitaciones. La **dependencia de datos de alta calidad** es uno de los mayores desafíos, ya que los modelos requieren conjuntos de datos extensos, bien etiquetados y balanceados para alcanzar un rendimiento óptimo, como lo menciona [72], además la **explicabilidad de los modelos** es una preocupación crítica; técnicas como Deep Learning suelen ser vistas como cajas negras, lo que dificulta la interpretación y comprensión de sus resultados, tal como señala [34], finalmente, el **costo elevado de implementación** y la necesidad de una infraestructura tecnológica robusta limitan la adopción de estas técnicas, especialmente en pequeñas organizaciones financieras [36].



**Figura 5.** Ventajas y Limitaciones de técnicas de IA

- **PI3. ¿Qué factores condicionan el éxito de la implementación de inteligencia artificial en la detección de fraudes financieros, como la calidad de los datos o la infraestructura tecnológica?**

El éxito de la implementación de inteligencia artificial (IA) en la detección de fraudes financieros está condicionado por varios factores críticos, siendo los más importantes la **calidad de los datos**, la **infraestructura tecnológica** y la **capacitación del personal especializado**. La **calidad de los datos** es esencial, ya que los modelos de IA dependen de conjuntos de datos bien etiquetados, balanceados y representativos, según [70], las técnicas como SMOTE (Synthetic Minority Oversampling Technique) han permitido abordar problemas de datos desbalanceados, mejorando la precisión de los modelos en más del 15%, sin embargo las organizaciones con datos incompletos o desactualizados enfrentan una disminución significativa en el rendimiento de las técnicas de IA.

En cuanto a la **infraestructura tecnológica**, los sistemas distribuidos, como Apache Spark y Hadoop, permiten procesar grandes volúmenes de datos en tiempo real, como se destaca en [36], estos entornos son esenciales para manejar las crecientes demandas computacionales de modelos avanzados como Redes Neuronales Convolucionales (CNN) y Redes Neuronales en Grafos (GNN), sin embargo, el costo de implementación y mantenimiento de esta infraestructura puede ser prohibitivo para instituciones más pequeñas [34]. Por último, la **capacitación del personal especializado** es indispensable para garantizar el éxito en la adopción de IA, según [40], la transformación de habilidades en los equipos contables y financieros ha mejorado la efectividad y reducido los errores en la aplicación de estas técnicas.

**Tabla 6.** Factores que condicionan el éxito en la implementación de IA

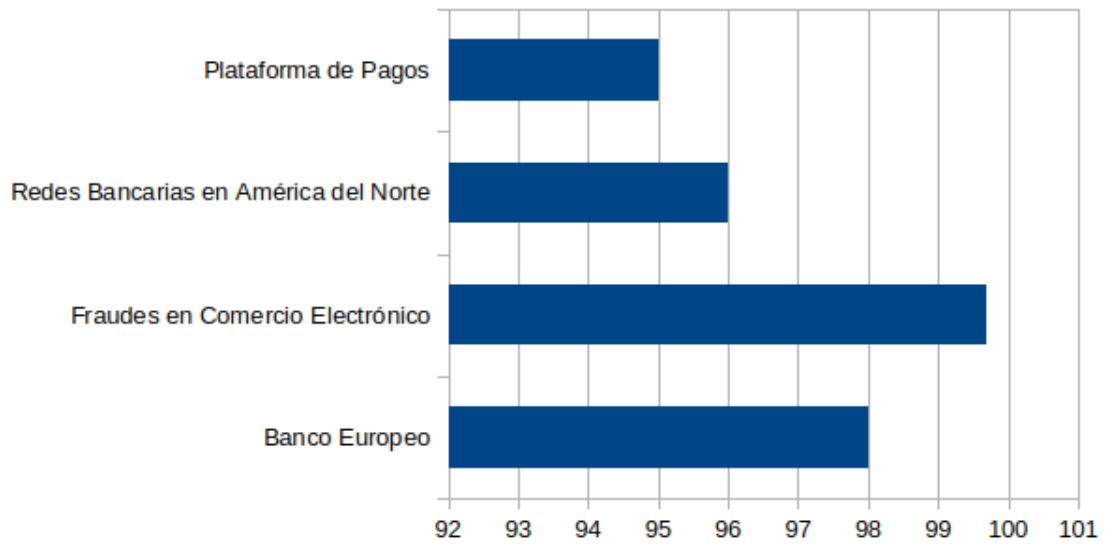
<b>Factor</b>	<b>Impacto Positivo (%)</b>	<b>Impacto Negativo (%)</b>
Calidad de los Datos	85%	15%
Infraestructura Tecnológica	75%	25%
Capacitación del Personal	70%	30%

- **PI4. ¿Qué casos documentados demuestran el impacto positivo de la inteligencia artificial en la reducción de fraudes**

Los casos documentados en la literatura evidencian que las técnicas de inteligencia artificial (IA) alcanzan altos niveles de precisión en la detección de fraudes financieros, el caso del **Banco Europeo** destaca por su precisión del 98%, lograda gracias a un sistema de detección en tiempo real que reduce significativamente los errores y tiempos de respuesta, de manera similar, en el ámbito del **comercio electrónico**, se alcanzó una precisión del 99.7% mediante el uso de Redes Neuronales Convolucionales (CNN), demostrando su efectividad en el análisis de transacciones globales.

Otros casos, como el de las **redes bancarias en América del Norte**, reportaron una precisión del 96%, reflejando los beneficios de la colaboración entre instituciones para mejorar los modelos de IA, finalmente, una **plataforma de pagos** logró adaptarse rápidamente a nuevos esquemas de fraude con una precisión del 95%, estos resultados subrayan que la IA no solo es confiable, sino también esencial para mitigar fraudes con alta exactitud, adaptándose a diferentes contextos y desafíos financieros.

### Precisión en Casos Documentados



**Figura 6.** Casos de impacto positivo de la IA

## IV. DISCUSIÓN Y CONCLUSIONES

### 4.1. Discusión

En esta investigación se ha explorado la aplicación de diversas técnicas de inteligencia artificial en la detección y prevención de fraudes financieros, los resultados obtenidos a partir de una revisión sistemática y las respuestas a las preguntas de investigación, entre las técnicas evaluadas, Random Forest y Gradient Boosting, incluyendo XGBoost y LightGBM, demostraron ser altamente eficaces, alcanzando precisiones superiores al 96% y áreas bajo la curva mayores al 99% en contextos de datos desbalanceados, estas técnicas sobresalen por su capacidad para identificar patrones complejos en grandes volúmenes de datos y adaptarse a esquemas de fraude emergentes, asimismo el aprendizaje profundo, particularmente mediante Redes Neuronales Convolucionales y Long Short-Term Memory, logró precisiones superiores al 99.7% con una alta tasa de detección en tiempo real, lo que subraya su ventaja en aplicaciones que requieren una respuesta rápida.

Por otra parte, las Redes Neuronales en Grafos se perfilan como una herramienta prometedora para modelar relaciones complejas entre transacciones financieras, estas redes incrementaron el área bajo la curva en un 10% en estudios centrados en patrones fraudulentos en redes, demostrando su capacidad para abordar estructuras de datos más sofisticadas, la evidencia también respalda que las técnicas de inteligencia artificial superan a los métodos tradicionales en precisión y en la reducción de falsos positivos. Por ejemplo, Gradient Boosting redujo los falsos positivos en un 87%, mientras que Random Forest demostró ser particularmente eficaz en contextos de transacciones desbalanceadas. Además, estas técnicas ofrecen una adaptación rápida a nuevos esquemas de fraude, una característica crítica en el dinámico entorno financiero actual.

No obstante, también se identificaron limitaciones significativas. La calidad y cantidad de datos son factores determinantes para el éxito de estas implementaciones, lo que resalta

la necesidad de contar con conjuntos de datos bien etiquetados y representativos. Además, la explicabilidad de los modelos, particularmente en técnicas de aprendizaje profundo, sigue siendo un desafío que afecta la confianza y la adopción de estas soluciones en sectores financieros. Finalmente, los costos elevados de implementación y mantenimiento de infraestructura limitan la adopción de estas tecnologías en organizaciones más pequeñas, el éxito de la implementación de inteligencia artificial en la detección de fraudes financieros está condicionado por la calidad de los datos, la infraestructura tecnológica y la capacitación del personal. Estudios recientes muestran que técnicas como SMOTE han mejorado la precisión de los modelos en más del 15% al abordar problemas de datos desbalanceados, por otro lado, plataformas distribuidas como Apache Spark y Hadoop han optimizado el procesamiento de datos en tiempo real, lo que resulta esencial para soportar modelos avanzados como Redes Neuronales en Grafos, sin embargo, estas soluciones requieren una inversión significativa en infraestructura y capacitación de personal.

Los casos documentados evidencian un impacto positivo significativo de la inteligencia artificial en la reducción del fraude financiero, por ejemplo un banco europeo logró una precisión del 98% mediante sistemas de detección en tiempo real, mientras que, en el comercio electrónico, las Redes Neuronales Convolucionales alcanzaron una precisión del 99.7%, demostrando su eficacia en escenarios globales, estas experiencias resaltan la importancia de fomentar la colaboración entre instituciones financieras y desarrolladores para implementar soluciones inclusivas y escalables. En síntesis, la investigación respalda que las técnicas de inteligencia artificial representan un avance significativo en la lucha contra el fraude financiero. Aunque persisten desafíos operativos y técnicos, como la calidad de los datos y los costos de implementación, los beneficios superan ampliamente las limitaciones, consolidando a la inteligencia artificial como una herramienta esencial para fortalecer la seguridad y confianza en los sistemas financieros.

#### **4.1. Conclusiones**

Esta investigación ha identificado un total de 51 estudios relacionados con el uso de técnicas de inteligencia artificial para la detección y prevención de fraudes financieros, confirmando un creciente interés en este campo. Estas técnicas han demostrado ser altamente efectivas, superando los métodos tradicionales al identificar patrones complejos y reducir falsos positivos. La revisión sistemática llevada a cabo permitió seleccionar los estudios más relevantes utilizando criterios estrictos de inclusión y exclusión, asegurando un análisis riguroso y representativo.

El análisis de los datos recopilados ha destacado que las técnicas de inteligencia artificial, como Random Forest, Gradient Boosting y Redes Neuronales Convolucionales, no solo mejoran la precisión, sino también permiten una detección más rápida y adaptativa. Sin embargo, se identifican limitaciones relacionadas con la calidad de los datos, la explicabilidad de los modelos y los costos asociados a su implementación, lo que subraya la importancia de invertir en tecnología y formación especializada.

Finalmente, los hallazgos de este estudio confirman que la inteligencia artificial representa una herramienta transformadora en la lucha contra el fraude financiero, capaz de fortalecer la confianza en los sistemas financieros globales. Para maximizar su impacto, es esencial fomentar la colaboración entre instituciones financieras y desarrolladores, garantizando que las soluciones sean inclusivas, transparentes y escalables en un entorno digital en constante evolución.



## V. REFERENCIAS

- [1] D. Ameijeiras Sánchez, O. Valdés Suárez y H. González Díez, «Algoritmos de detección de anomalías con redes profundas. Revisión para detección de fraudes bancarios,» *ScienceDirect*, vol. 15, nº 1, pp. 244-264, 2021.
- [2] Asociación argentina de ética y compliance, «Reporte sobre el fraude ocupacional municipal, ACFE 2024,» ACFE, Argentina, 2024.
- [3] T. Awosika, R. Mani Shukla y B. Pranggono, «Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection,» *IEEEExplore*, vol. 1, nº 1, pp. 10-30, 2023.
- [4] «Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review,» *IEEEExplore*, vol. 10, nº 1, pp. 1-15, 2022.
- [5] A. Abdulalem , R. Shukor Abd , O. Siti Hajar , E. E. Taiseer Abdalla , D. Arafat Al, N. Maged , E. Tusneem , E. Hashim y S. Abdu , «Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review,» *ScienceDirect*, vol. 1, nº 12, pp. 3-13, 2022.
- [6] F. Alvarez, «Machine Learning en la detección de fraudes de comercio electrónico aplicado a los servicios bancarios (Machine Learning en la detección de fraudes de comercio electrónico aplicado a los servicios bancarios),» *Scopus*, vol. 1, nº 1, pp. 81-95, 2020.
- [7] R. C. Dávila-Morán, R. A. Castillo-Sáenz, A. R. Vargas-Murillo, L. Velarde Dávila, E. García Huamantumba, C. F. García Huamantumba, R. F. Pasquel Cajas y C. E. Guanilo Paredes, «Aplicación de Modelos de Aprendizaje Automático en la Detección de Fraudes en Transacciones Financieras,» *Scopus*, vol. 1, nº 2, pp. 3-10, 2023.
- [8] C. A. Benites Ocampo, «Detectando el Fraude con Inteligencia Artificial: Una Perspectiva Avanzada en Auditoría Forense,» *La Junta*, vol. 2, nº 6, pp. 13-40, 2023.
- [9] C. A. Rayo Mondragon, «Prototipo De Detección De Fraudes Con Tarjetas De Crédito

Basado En Inteligencia Artificial Aplicado A Un Banco Peruano,» *Scopus*, vol. 1, nº 1, pp. 1-11, 2020.

- [10] L. R. Taboada Cornetero, *Modelo De Seguridad De La Información Para Contribuir En La Mejora De La Seguridad De Los Activos De Información Financiera De Las Unidades De Gestión Educativa Local De Lambayeque*, Chiclayo: UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO, 2021.
- [11] IBM, «An introduction to deep learning,» 09 noviembre 2020. [En línea]. Available: <https://developer.ibm.com/learningpaths/get-started-with-deep-learning/an-introduction-to-deep-learning/>. [Último acceso: 09 mayo 2023].
- [12] J. B. SANCHO, *Machine Learning y Deep Learning*, Bogotá: Bogotá: Ediciones, 2020.
- [13] j. Bobadilla, «Machine Learning y Deep Learning: Usando Python, Scikit y Keras,» 1 ed., madrid, RE-MA Editorial, 2020.
- [14] «Education, Big Data and Artificial Intelligence: Mixed methods in digital platforms,» *Scopus*, vol. 28, nº 1, p. 52, 2020.
- [15] D. D. Figaredo, «Big Data, analítica del aprendizaje y educación basada en datos (Big Data, Learning Analytics & Data-driven Education),» *SSRN*, vol. 1, nº 1, p. 19, 2018.
- [16] L. R. Calcagni, «Redes Generativas Antagónicas y sus aplicaciones,» *Univercidad nacional de la plata*, vol. I, 2014.
- [17] aws, «¿Qué es una GAN?,» 2023. [En línea]. Available: <https://aws.amazon.com/es/what-is/gan/>. [Último acceso: 14 julio 2024].
- [18] Unir, «¿Qué es el transfer learning y qué ventajas tiene?,» 02 noviembre 2023. [En línea]. Available: <https://www.unir.net/ingenieria/revista/transfer-learning/>. [Último acceso: 12 mayo 2024].
- [19] A. H. A. H. M. M. A. M. Madkour, «Dynamic Classification Ensembles for Handling Imbalanced Multiclass Drifted Data Streams,» *Scopus*, vol. 670, nº 120555, p. 49, 2024.

- [20] L. N. Z. Morales, «Ensemble Learning,» *Creative Commons*, vol. 1, nº 1, p. 19, 2024.
- [21] G. P. G. ´. alez, «Deteccion de transacciones fraudulentas en tarjetas ´,» *Universidad de los Andes*, vol. 1, nº 1, pp. 1-5, 2023.
- [22] C. C. Noble y D. J. Cook, «Graph-Based Anomaly Detection," Department of Computer Science Engineering, University of Texas at Arlington,» *University of Texas at Arlington*, 2000.
- [23] E. RODRÍGUEZ PÉREZ, «Detección de Anomalías Basada en Grafos,» *UNIVERSIDADPOLITÉCNICA DEMADRID*, pp. 23-27, 2020.
- [24] J. D. Espitia Moreno, «Aprendizaje federado y privacidad diferencial: una aplicación en bases de datos clínicos,» *Universidad de los Andes*, vol. 1, nº 1, pp. 1-9, 2023.
- [25] E. D. Angulo Madrid, «Entrenamiento de modelos de clasificación con aprendizaje federado preservando la privacidad de los datos,» *Universidad del Norte*, vol. 1, nº 1, pp. 1-11, 2022.
- [26] A. P. David Byrd, «Computación privada diferencial y segura entre múltiples partes para el aprendizaje federado en aplicaciones financieras,» *ArXiv*, vol. 1, nº 1, pp. 1-13, 2020.
- [27] W. G. B. Morales, «Análisis de Prisma como Metodología para Revisión Sistemática: una Aproximación General.,» *Universidad Nacional Autónoma de Nicaragua, Managua.*, vol. 8, nº 1, p. 22, 2022.
- [28] W. L. Junwen Zhu, «A tale of two databases: the use of Web of Science and Scopus in academic papers,» *Researchgate*, vol. 1, nº 1, pp. 1-10, 202.
- [29] O. V. A. E. O. O. Oluwaseun Isaac Odufisan, «Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria,» *ScienceDirect*, vol. 7, nº 1, pp. 1-10, 2025.
- [30] S. A. G. J. Y. Waleed Hilal, «Fraude financiero: una revisión de las técnicas de detección de anomalías y los avances recientes,» *ScienceDirect*, vol. 193, nº 1, pp. 2-

8, 2022.

- [31] A. H. A. H. A. Ali, «An enhanced AI-based model for financial fraud detection,» *Scopus*, vol. 10, n° 11, pp. 114-121, 2025.
- [32] L. M. A. A. Abakarim Youness, «An efficient real time model for credit card fraud detection based on deep learning,» *Scopus*, vol. 1, n° 30, pp. 10-23, 2020.
- [33] M. K. A. B. Asma Cherif, «Credit card fraud detection in the era of disruptive technologies: A systematic review,» *ScienceDirect*, vol. 35, n° 1, pp. 145-174, 2023.
- [34] H. L. Z. X. J. Q. Ying Zhou, «A user-centered explainable artificial intelligence approach for financial fraud detection,» *ScienceDirect*, vol. 58, n° 1, pp. 2-21, 2023.
- [35] Q. S. S. B. F. Ziyue Wang, «AI Empowers Data Mining Models for Financial Fraud Detection and Prevention Systems,» *ScienceDirect*, vol. 243, n° 1, pp. 891-899, 2024.
- [36] F. X. S. G. J. W. Zhou Hangjun, «A distributed approach of big data mining for financial fraud detection in a supply chain,» *Scopus*, vol. 1, n° 1, pp. 10-33, 2020.
- [37] G. H. B. H. M. Y. Dhieb Najmeddine, «A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement,» *Scopus*, vol. 1, n° 1, pp. 2-33, 2020.
- [38] L. A. Garcia-Segura, «The role of artificial intelligence in preventing corporate crime,» *ScienceDirect*, vol. 5, n° 1, pp. 13-33, 2024.
- [39] P. K. Surendranadha Reddy Byrapu Reddy, «Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics,» *ScienceDirect*, vol. 33, n° 1, pp. 1-22, 2024.
- [40] J. A. M. N. Bou Reslan Fadi, «Assessing the Transformative Impact of AI Adoption on Efficiency, Fraud Detection, and Skill Dynamics in Accounting Practices,» *Scopus*, vol. 1, n° 1, pp. 11-34, 2024.
- [41] M. M. Ismail, «Enhancing Enterprise Financial Fraud Detection using Machine Learning,» *Scopus*, vol. 1, n° 1, pp. 4-22, 2024.

- [42] A. V. Anastasiia Izotova, «Comparison of Poisson process and machine learning algorithms approach for credit card fraud detection,» *ScienceDirect*, vol. 33, n° 1, pp. 721-726, 2021.
- [43] M. A. A. H. Y. H. Xinyi Zheng, «Data mining algorithm in the identification of accounting fraud by,» *ScienceDirect*, vol. 1, n° 1, pp. 20-34, 2024.
- [44] A. K. Ivan Vorobyev, «Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models,» *ScienceDirect*, vol. 120, n° 1, pp. 22-55, 2022.
- [45] L. L. R. J. W. H. D. L. Qingfeng Zeng, «NNEnsLeG: A novel approach for e-commerce payment fraud detection using ensemble learning and neural networks,» *ScienceDirect*, vol. 62, n° 1, pp. 2-32, 2024.
- [46] D.-A. H. M. K. S. Dehghani Jaber, «Artificial intelligence and data mining techniques: Applications in financial fraud detection,» *Scopus*, vol. 1, n° 1, pp. 33-56, 2024.
- [47] P. Juyal, «Using Deep and Machine Learning Techniques to Spot Credit Card Fraud,» *Scopus*, vol. 1, n° 1, pp. 752 - 758, 2024.
- [48] L. K. Choi Dahee, «An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation,» *Scopus*, vol. 1, n° 1, pp. 4-18, 2020.
- [49] S. R. R. Tanouz D, «Credit card fraud detection using machine learning,» *Scopus*, vol. 1, n° 1, pp. 967 - 972, 2022.
- [50] S. H. T. V. Bart Baesens, «Data engineering for fraud detection,» *ScienceDirect*, vol. 150, n° 1, pp. 7-21, 2021.
- [51] S. K. K. Asha RB, «Credit card fraud detection using artificial neural network,» *ScienceDirect*, vol. 2, n° 1, pp. 35-41, 2021.
- [52] A. I. H. A. M. K. S. A. Asma Cherif, «Encoder–decoder graph neural network for credit card fraud detection,» *ScienceDirect*, vol. 36, n° 1, pp. 10-31, 2024.

- [53] I. N. S. M. H. Sumaya S. Sulaiman, «Credit Card Fraud Detection Using Improved Deep Learning Models,» *ScienceDirect*, vol. 1, n° 1, pp. 1049-1069, 2024.
- [54] J. G. X. L. H. Y. Xinzhi Wang, «DyHDGE: Dynamic heterogeneous transaction graph embedding for safety-centric fraud detection in financial scenarios,» *ScienceDirect*, vol. 5, n° 1, pp. 486-497, 2024.
- [55] I. K. S. S. Fazal Wahab, «Credit card default prediction using ML and DL techniques,» *ScienceDirect*, vol. 4, n° 1, pp. 293-306, 2024.
- [56] C. Z. Feifen Shi, «Enhancing financial fraud detection with hierarchical graph attention networks: A study on integrating local and extensive structural information,» *ScienceDirect*, vol. 58, n° 1, pp. 10-33, 2023.
- [57] J. S. Guoxiang Tong, «Financial transaction fraud detector based on imbalance learning and graph neural network,» *ScienceDirect*, vol. 149, n° 1, pp. 11-56, 2023.
- [58] R. H. D. L. L. R. W. H. Y. Z. Junhang Wu, «A GNN-based fraud detector with dual resistance to graph disassortativity and imbalance,» *ScienceDirect*, vol. 669, n° 1, pp. 33-76, 2024.
- [59] B. F. Y. T. Z. T. Z. S. A. L. Yunqi Li, «Abnormal Detection of Financial Fraud in Listed Companies Based on Deep Learning,» *ScienceDirect*, vol. 242, n° 1, pp. 55-99, 2024.
- [60] A. S. M. H.R. Ranganatha, «Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3d Quasi-Recurrent Neural network and blockchain technologies,» *ScienceDirect*, vol. 260, n° 1, pp. 44-77, 2025.
- [61] N. K. K. P. K. K. S. K. d. D. N. S. S. D. V. Mahalakshmi, «The Role of implementing Artificial Intelligence and Machine Learning Technologies in the financial services Industry for creating Competitive Intelligence,» *ScienceDirect*, vol. 56, n° 1, pp. 2252-2255, 2022.
- [62] M. F. A. A. B. M. T. Rihab Najem, «Artificial Intelligence for Digital Finance, Axes and Techniques,» *ScienceDirect*, vol. 203, n° 1, pp. 633-638, 2022.

- [63] R. T. N. C. G. P. H. W. M. D. Felipe Dias Paiva, «Decision-making for financial trading: A fusion approach of machine learning and portfolio selection,» *ScienceDirect*, vol. 115, n° 1, pp. 635-655, 2020.
- [64] K. N. Chandana Gouri Tekkali, «Assessing CNN's Performance with Multiple Optimization Functions for Credit Card Fraud Detection,» *ScienceDirect*, vol. 235, n° 1, pp. 2035-2042, 2024.
- [65] M. L. Y. W. Xuting Mao, «Using GNN to detect financial fraud based on the related party transactions network,» *ScienceDirect*, Vols. %1 de %2351-358, n° 1, p. 214, 2022.
- [66] S. N. Y. M. G. Swathi Moturi, «Fraud Detection in Digital and Netbanking Using Machine Learning,» *Scopus*, vol. 1, n° 1, pp. 770 - 776, 2024.
- [67] N. Z. M. E. N. Olubusola Odeyemi, «Reviewing the role of AI in fraud detection and prevention in financial services,» *Scopus*, vol. 1, n° 1, pp. 19-55, 2024.
- [68] R. C. V. R. P. B. M. Narsimha B, «Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application,» *Scopus*, vol. 1, n° 1, pp. 20-34, 2022.
- [69] S. G. F. S. W. L. H. J. Zhou Hangjun, «Internet Financial Fraud Detection Based on a Distributed Big Data Approach with Node2vec,» *Scopus*, vol. 1, n° 1, pp. 66-109, 2021.
- [70] S. M. H. I. N. I. Sumaya Saad Sulaiman, «Credit Card Fraud Detection Challenges and Solutions :A Review,» *Scopus*, vol. 1, n° 1, pp. 44-88, 2024.
- [71] D. Y. S. W. H. S. Zhaowei Liu, «Adaptive multi-channel Bayesian graph attention network for IoT transaction security,» *ScienceDirect*, vol. 10, n° 1, pp. 631-644, 2024.
- [72] «Application of machine learning models and artificial intelligence to analyze annual financial statements to identify companies with unfair corporate culture,» *ScienceDirect*, vol. 176, n° 1, pp. 3037-3046, 2020.
- [73] H. G. Amirreza Tajally, «Uncertainty-Aware Credit Card Fraud Detection Using Deep

Learning,» *Scopus*, vol. 1, nº 1, pp. 38-99, 2021.

[74] F. B. T. Philip Olaseni Shoetan, «TRANSFORMANDO LA DETECCIÓN DE FRAUDES EN FINTECH CON ALGORITMOS AVANZADOS DE INTELIGENCIA ARTIFICIAL,»

*Scopus*, vol. 6, nº 4, pp. 10-77, 2024.

[75] M. Shohreh Yazdani, «Presenting a Model for Financial Reporting Fraud Detection using Genetic Algorithm,» *Scopus*, vol. 1, nº 1, pp. 377 - 392, 2021.

[76] I. C. M. I. B. Mircea Constantin Şcheau, «Privacy Intrusiveness in Financial-Banking Fraud Detection,» *Scopus*, vol. 9, nº 6, pp. 88-100, 2021.

[77] P. M. Mimusa Azim Mim, «A soft voting ensemble learning approach for credit card fraud detection,» *ScienceDirect*, vol. 10, nº 3, pp. 22-88, 2024.

[78] M. F. P. Michael Geraldin Wijaya, «Comparative Analysis of Machine Learning Algorithms and Data Balancing Techniques for Credit Card Fraud Detection,» *ScienceDirect*, vol. 245, nº 1, pp. Pages 677-688, 2024.

[79] N. A. FAWAZ KHALED ALARFAJ, «Credit Card Fraud Detection Using,» *Science Direct*, vol. 10, nº 1, pp. 77-99, 2022.



## ANEXOS

### Anexo 1. Reporte de similitud (Turnitin)

# Mondragón Fernández Alex Yarango Farro Darwin ...

## Revisión sistemática sobre el uso de la Inteligencia Artificial para la detección y prevención de fr

- My Files
- My Files
- Universidad Señor de Sipan

### Detalles del documento

Identificador de la entrega  
trn:oid:::26396:424345723

Fecha de entrega  
28 ene 2025, 11:27 a.m. GMT-5

Fecha de descarga  
28 ene 2025, 11:31 a.m. GMT-5

Nombre de archivo  
Turnitin YARANGO\_MONDRAGON\_TRABAJO\_INVESTIGACIÓN.docx

Tamaño de archivo  
447.4 KB

56 Páginas

9,151 Palabras

54,972 Caracteres



Página 2 of 65 - Descripción general de integridad

Identificador de la entrega trn:oid:::26396:424345723

## 17% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

### Filtrado desde el informe

- ▶ Bibliografía
- ▶ Texto mencionado
- ▶ Coincidencias menores (menos de 8 palabras)

### Fuentes principales

- 11% Fuentes de Internet
- 5% Publicaciones
- 14% Trabajos entregados (trabajos del estudiante)

### Marcas de integridad

#### N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Anexo 02. Enlace de drive de artículos seleccionados:

<https://drive.google.com/drive/folders/15BWMX3qwOAKHCNF-xrGq3YZc1pUR6GmE?usp=sharing>