Revisión sistemática de literatura de redes neuronales para la detección de fraudes en transacciones financieras

Urdánigo Saltos Cristhian Adrián
Universidad Técnica De Manabí (UTM)
curdanigo9906@utm.edu.ec

Alcívar Cevallos Roberth Abel
Universidad Técnica De Manabí (UTM)
roberth.alcivar@utm.edu.ec

DOI: https://doi.org/10.56124/encriptar.v8i15.014

Resumen

Actualmente las transacciones financieras juegan un papel fundamental en nuestro día a día. Este artículo presenta una revisión sistemática de literatura (SLR) sobre el uso de redes neuronales para detectar, predecir y prevenir fraudes en transacciones financieras. La primera parte de esta investigación se enfoca en la recopilación de datos, la cual se realizó siguiendo la metodología PRISMA. Se recopiló un conjunto de datos basados en estudios e investigaciones con el objetivo de obtener resultados que puedan proporcionar una visión clara sobre el uso de redes neuronales para la detección de fraudes en transacciones financieras. Durante el proceso de investigación se demuestra que las Redes Neuronales Generativas (GAN) y las Redes Neuronales Artificiales (ANN) son las más utilizadas a la hora de detectar y predecir fraudes en transacciones financieras, Además, se evidencia que las redes neuronales más eficientes para la detección de fraude en transacciones financieras son las Redes Neuronales Recurrentes alcanzando una precisión de 98.71% y las redes neuronales generativas (GAN) con una precisión de 97.1%. Estos resultados indican claramente que las redes neuronales son altamente eficientes para detectar y predecir fraude en transacciones financieras. En este estudio se demuestra el progreso significativo que han tenido las redes neuronales, mejorando de manera notable la precisión en la detección de fraudes financiero. Estos avances han permitido reducir el riesgo de fraude y ofrecer soluciones más eficientes en el ámbito financiero. Los resultados obtenidos de esta investigación proporcionan una guía valiosa para investigadores y profesionales en el campo de la ciberseguridad.

Palabras clave: Redes neuronales, Detección de fraudes, Transacciones financieras, Metodología PRISMA, Ciberseguridad.

Systematic literature review of neural networks for fraud detection in financial transactions.

ABSTRACT

Currently, financial transactions play a fundamental role in our daily lives. This article presents a systematic literature review (SLR) on the use of neural networks to detect, predict, and prevent fraud in financial transactions. The first part of this research focuses on data collection, which was conducted following the PRISMA methodology. A dataset was compiled based on studies and research with the aim of obtaining results that can provide a clear insight into the use of neural networks for fraud detection in financial transactions. During the research process, it is demonstrated that Generative Adversarial Networks (GANs) and Artificial Neural Networks (ANNs) are the most commonly used for detecting and predicting fraud in financial transactions. Furthermore, it is evident that the most efficient neural networks for fraud detection in financial transactions are Recurrent Neural Networks, achieving an accuracy of 98.71%, and Generative Adversarial Networks (GANs) with an accuracy of 97.1%. These results clearly indicate that neural networks are highly effective in detecting and predicting fraud in financial transactions. This study demonstrates the significant progress that neural networks have made, notably improving accuracy in financial fraud detection. These advancements have allowed for a reduction in fraud risk and provided more efficient solutions in the financial sector. The results obtained from this research provide a valuable guide for researchers and professionals in the field of cybersecurity.

Keywords: Neural networks, Fraud detection, Financial transactions, PRISMA Methodology, Cybersecurity.

1. INTRODUCCION

En la actualidad, las transacciones financieras son una parte integral de la vida cotidiana de las personas. Sin embargo, a medida que evolucionan los métodos de pago, también lo hacen las tácticas fraudulentas. Según estudios recientes, se estima que el fraude financiero cuesta a las empresas miles de millones de dólares anuales, afectando no solo a las instituciones financieras, sino también a los consumidores y a la economía global en general [1]. La detección precisa de fraudes en transacciones financieras se vuelve esencial para salvaguardar los recursos y la seguridad económica. Por tanto, es necesario desarrollar tecnologías avanzadas y métodos predictivos, centrándose en la aplicación de redes neuronales para reducir el

riesgo de manera eficiente y oportuna, y preservar la integridad del sistema financiero [2].

La identificación de irregularidades en las transacciones es crucial para proteger los recursos económicos. Sin embargo, las técnicas tradicionales de detección a menudo son insuficientes, dado que no pueden adaptarse rápidamente a las nuevas formas de fraude que surgen. Este vacío en la literatura destaca la necesidad de investigar tecnologías avanzadas y métodos predictivos, especialmente en lo que respecta a las redes neuronales, que han demostrado tener un potencial prometedor en la mejora de la precisión en la detección de anomalías [3].

La tarea de detección de fraude no es un tema fácil de resolver, teniendo en cuenta las múltiples modalidades y evolución rápida que esta problemática ha tenido en la actualidad. El aumento significativo del fraude, su complejidad cada vez mayor y su especialización hacen que los recursos utilizados por parte de las organizaciones para combatirlos sean cada vez más significativos [4].

Las instituciones financieras enfrentan de manera constante el riesgo de sufrir pérdidas económicas debido a transacciones fraudulentas. Este desafío impulsa a mejorar de manera continua sus procesos con el fin de gestionar y prevenir eficazmente el fraude. A pesar de los recientes avances en inteligencia artificial y aprendizaje automático, existe una falta de estudios que analicen de manera integral las capacidades de diversas arquitecturas de redes neuronales para enfrentar el problema del fraude en transacciones financieras [5].

En vista de estos desafíos, este estudio de Revisión Sistemática de la Literatura (RSL) se centrará en identificar y analizar los tipos de redes

neuronales más efectivos para la detección de fraude financiero. A través de este enfoque riguroso y metodológico, se proporciona una comprensión más profunda de las fortalezas y debilidades de estos algoritmos, lo que ayudará a futuras investigaciones en el campo de la ciberseguridad.

2. METODOLOGIA

En este trabajo de investigación se exploran diversos modelos de redes neuronales que permiten la detección de fraude en transacciones financieras atreves de una revisión sistemática de literatura. En este contexto se utiliza la metodología PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) aplicada por [6]. Esta implica un proceso riguroso y estructurado para recopilar y analizar la información relevante con el propósito de explorar exhaustivamente el estado actual del uso de las redes neuronales en la detección de fraudes en transacciones financieras.

Este tipo de investigación analítica proporciona una estructura metodológica rigurosa que permite la identificación, evaluación y síntesis de la evidencia disponible en la literatura científica relevante. La cual está compuesta por los siguientes pasos:

- Planificación
- Preguntas de investigación
- Selección de estudios
- Exploración de documentos

2.1 PLANIFICACIÓN:

En esta etapa, se detallan las cadenas de búsqueda utilizadas para obtener información relevante sobre la aplicación de redes neuronales en la detección de fraudes en transacciones financieras. Estas cadenas de búsqueda fueron formuladas de manera rigurosa, incorporando términos clave que contribuyeron significativamente a los resultados de esta investigación. Se llevó a cabo la búsqueda en inglés y en español, utilizando operadores booleanos para refinar los resultados.

Cadenas de búsqueda utilizadas en los gestores de base de datos académicas

Tabla I. Cadena de búsqueda usada para cada Base de Datos Académica.

Cadenas de búsqueda	Bases de datos académicas
- ("Detección De Fraude" OR "Redes Neuronales" AND "Transacciones Financieras")	Scielo
- ("Financial transactions" OR "transaction anomalies" OR "neural networks" OR "artificial neural networks")) - "Neural networks" AND "fraud detection" AND "financial transactions" AND (application OR method OR model) - ("Inteligencia Artificial" OR "Algoritmos de IA") AND ("Fraude Financieros")	Scopus
- ("Neural network" AND "fraud detection" AND (efficiency OR effectiveness OR performance))	IEEE

- ("Artificial Intelligence Algorithms" OR "Machine Learning") AND ("Cybercrime Detection" OR "Cybercrimes")	
- ("Detección De Fraude" OR "Aprendizaje Automático" OR "Redes Neuronales Convolucionales" AND "Evaluación De Rendimiento")	Repositorios Institucionales
- "Neural networks" OR "deep learning" OR "machine learning" OR "artificial intelligence" OR "computational intelligence")	Dialnet

Esta búsqueda abarcó estudios primarios publicados en el período comprendido entre el 2018 y 2024. Durante este proceso, se recopilo los resultados de dichos estudios, centrándose en las técnicas de Redes Neuronales utilizadas en la detección de fraude.

2.2 PREGUNTAS DE INVESTIGACION:

Las preguntas de investigación desempeñaron un papel crucial en la identificación de recursos relevantes, así como en la recopilación de datos y herramientas necesarias para llegar a conclusiones sólidas de esta investigación, que incluyen: (a) Redes Neuronales, (b) Detección de Fraudes, (c) Transacciones Financieras, (d) Fraude Financiero.

RQ1. ¿Cuáles son las principales técnicas de redes neuronales utilizadas en la detección de fraude en transacciones financieras?

RQ2. ¿Cuál es el nivel de eficiencia de las técnicas de redes neuronales en la detección de fraude financiero según los resultados obtenidos en casos prácticos?

RQ3. ¿Cómo están evolucionando las técnicas de redes neuronales para abordar los desafíos y delitos emergentes en las instituciones financieras?

2.3 SELECCIÓN DE ESTUDIOS:

Con el objetivo de mejorar la eficacia de las búsquedas, se implementaron criterios de selección, tanto para incluir como para excluir, los cuales involucraron la evaluación del título, la introducción y la conclusión de cada documento identificado.

Estos criterios se encuentran especificados en la tabla II. La aplicación de este protocolo de búsqueda y selección facilitó la identificación y elección de los documentos más relevantes en relación con el tema de investigación.

Criterios de selección:

Tabla II. Criterios de exclusión e inclusión.

Criterios de inclusión	Criterios de exclusión
Documentos donde se utilizan métodos/algoritmos basados en redes neuronales para la detección de Fraudes Financieros.	Documentos donde no se mencionen Redes Neuronales, Delitos Informáticos y Fraudes Financieros.
Documentos de acceso libre	Estudios no accesibles
Estudio a partir del 2018.	Documentos sin rigor científico, y estudios Duplicados.
Estudios en idiomas español e ingles	Investigaciones previas al 2018.

2.4 EXPLORACION DE DOCUMENTOS:

Los resultados más relevantes de esta investigación se presentan en la (Figura 1). Este proceso de revisión se centró principalmente en el período

que abarca desde 2018 hasta 2024.

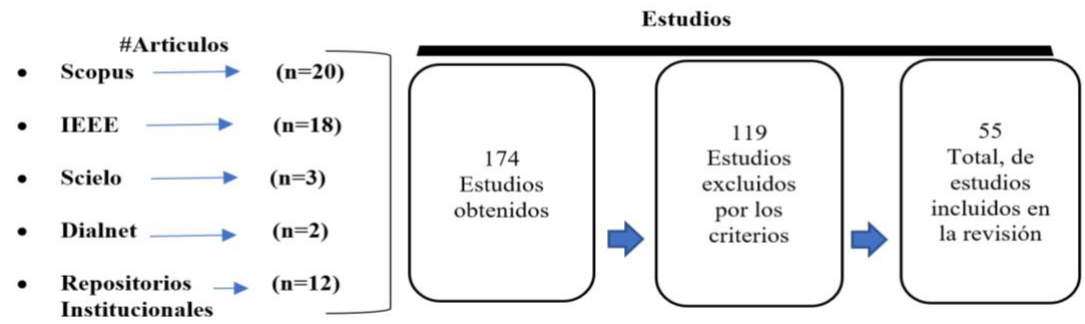

Figura 1. Flujo de búsqueda y selección de artículos

2.5 REVISIÓN:

En la etapa inicial de recopilación de datos, se realizó una búsqueda exhaustiva en cuatro bases de datos digitales: Scopus, IEEE, Scielo, Dialnet, también se encontró información valiosa en repositorios universitarios. Los documentos recopilados en la fase preliminar de esta investigación, detalladas en la (Figura 2), representan una amplia colección de documentos relevantes para el tema de estudio.

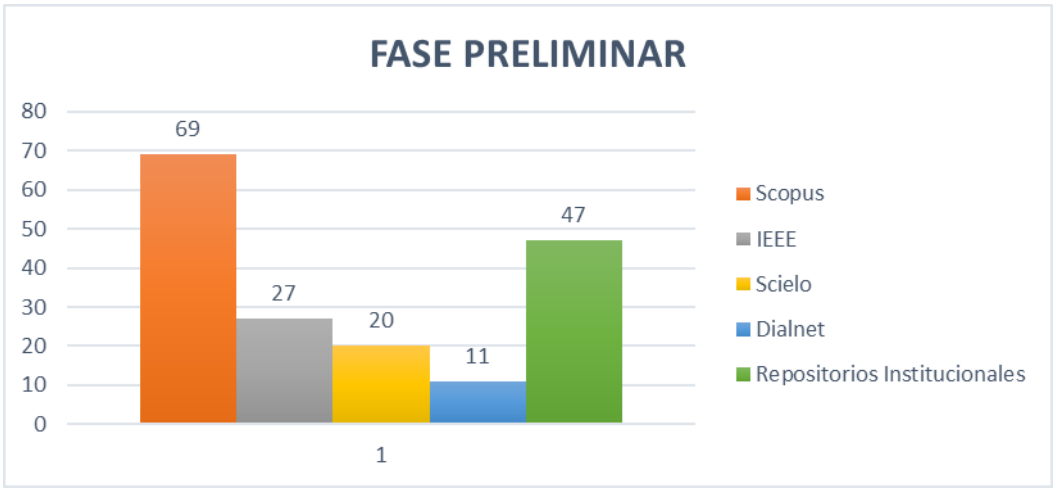

Figura 2. Artículos encontrados en las distintas bases de datos seleccionadas

Considerando la extensión de este conjunto de documentos, era necesario realizar un filtrado más estricto con el fin de asegurar que los trabajos elegidos estuvieran estrechamente vinculados a las tendencias de las técnicas de redes neuronales en la detección de fraude financiero. Este paso resultó ser crucial para mantener la precisión y relevancia del estudio. En consecuencia, se llevaron a cabo los criterios de inclusión y exclusión diseñados para depurar los documentos que no guardaban pertinencia con el tema de investigación. El impacto de este proceso de filtración se refleja claramente en la (Figura 3), donde el número de documentos seleccionados experimentó una reducción significativa: Scopus con 20 documentos, le sigue IEEE con 15, Scielo con 3 y Dialnet con 2, y otros artículos que fueron encontrado en revistas institucionales con 12 documentos, con un total de 52 estudios.

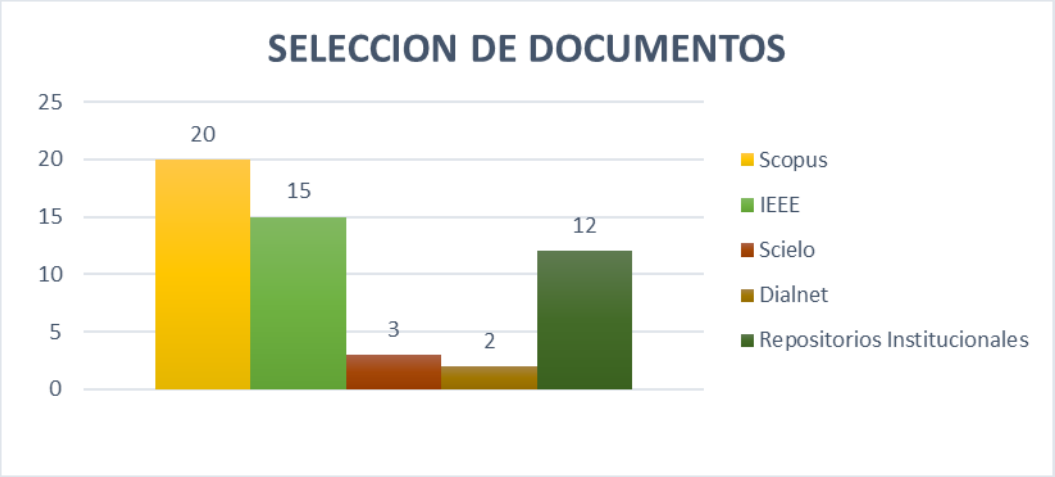

Figura 3. Artículos relevantes seleccionados

La notable disminución en la cantidad de documentos no sugiere una falta de materiales pertinentes, sino más bien evidencia la eficacia de los criterios de inclusión y exclusión implementados. La aplicación meticulosa de estos criterios aseguró la selección únicamente de los documentos más

relevantes para el análisis final, mejorando así la calidad y pertinencia de los descubrimientos en este estudio. Este proceso de búsqueda y selección facilitó la identificación de documentos más apropiados para examinar las tendencias actuales en las técnicas de redes neuronales aplicadas en la detección de fraude financiero. A pesar de la reducción en la cantidad de documentos, la relevancia y calidad de los seleccionados proporcionan un conjunto sólido de evidencias para el análisis. Entre los 43 documentos analizados, se emplearon diversos tipos de redes para detectar fraude en transacciones financieras.

3. RESULTADOS:

RQ1. ¿Cuáles son las principales técnicas de redes neuronales utilizadas en la detección de fraude en transacciones financiera?

En este estudio, se observa que la detección de fraude en transacciones financieras involucra una diversidad de enfoques en el ámbito de las redes neuronales, el cual ha tenido como finalidad minimizar esta clase de delitos financieros, de acuerdo a los estudios, las principales técnicas de redes neuronales utilizadas para abordar esta problemática incluyen las siguientes: Las Redes Generativas Adversarias (GAN) se destacaron como las más utilizadas, apareciendo en 12 estudios. Le siguen las Redes Neuronales Artificiales (ANN), que se encontraron en 8 estudios. Las Redes Neuronales Recurrentes (RNN), las Redes Neuronales Convolucionales (CNN) y las LSTM (Long Short-Term Memory) se mencionaron en 4 estudios cada una. Finalmente, los Autoencoders (AE) se identificaron en 4 estudios. La Figura 4 muestra la frecuencia de aparición de cada una de estas técnicas en la literatura revisada [7], [8], [9], [10].

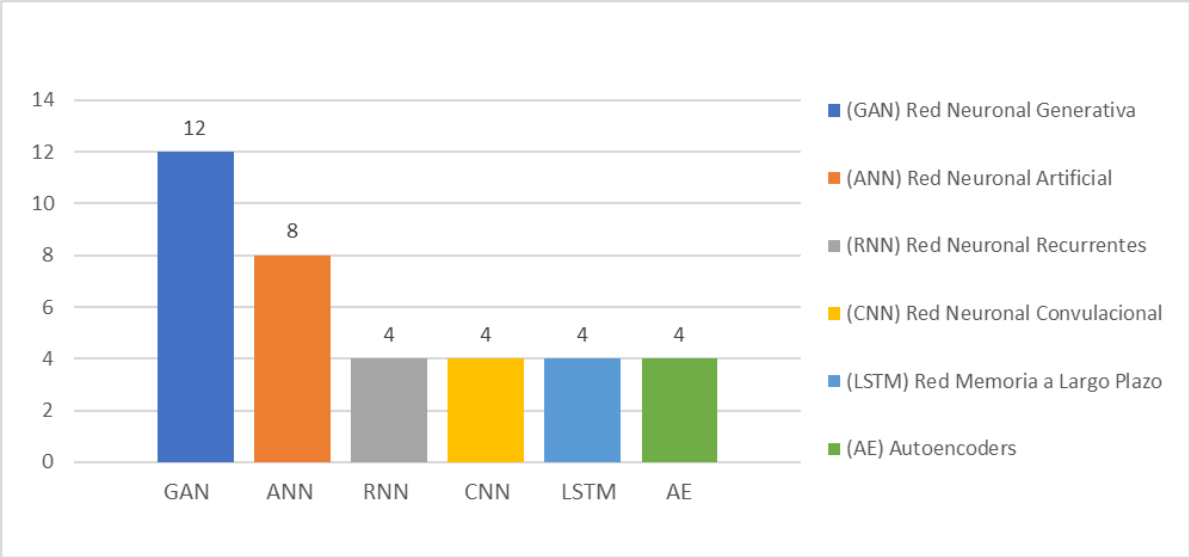

Figura 4. Redes neuronales más utilizadas en este estudio

Los resultados de esta investigación demuestran que las redes neuronales generativas (GAN) se destacaron, siendo estas las más utilizadas a la hora de detectar fraudes en transacciones financieras, Su alta adopción se debe a su capacidad de generar datos sintéticos realistas permitiendo a los modelos aprender de una variedad de escenarios. Posteriormente, Edu (2024), sostiene que: Las redes neuronales artificiales (ANN) son también altamente utilizadas debido a su capacidad para modelar relaciones complejas y manejar datos secuenciales. Estas pueden ser utilizadas para clasificar transacciones como legítimas o fraudulentas basándose en características como el monto, la ubicación, el historial del usuario y otros factores relevantes. Su capacidad para aprender patrones complejos a partir de grandes volúmenes de datos las hace efectivas para identificar comportamientos inusuales que podrían indicar fraude. Así mismo las técnicas (RNN), (CNN), (LSTM) y autoencoders (AE) complementan estas estrategias, ofreciendo enfoques adicionales para mejorar la detección de fraudes. Al combinar estas arquitecturas, se puede crear un sistema robusto con el objetivo de minimizar y reducir el riesgo de fraudes en

transacciones financieras, Las (CNN) pueden extraer características relevantes, las (LSTM) y (RNN) pueden analizar patrones temporales y secuenciales en los datos, y los autoencoders (AE) pueden identificar transacciones inusuales calculando en la reconstrucción de datos. Esta integración permite una detección más precisa y efectiva de actividades fraudulentas, mejorando la seguridad en el ámbito financiero [11], [12].

RQ2. ¿Cuál es el nivel de eficiencia de las técnicas de redes neuronales más utilizadas en la detección de fraude financiero según los resultados obtenidos en casos prácticos?

El nivel de eficiencia de las técnicas basadas en redes neuronales para la detección de fraude financiero, se puede visualizar en la (Tabla III). Esta tabla recopila los resultados de varios estudios. En esta investigación se realizó una búsqueda exhaustiva de documentos relevantes, con el objetivo de encontrar aquellos tipos de redes neuronales más utilizados para la detección de fraude en transacciones financieras. Este trabajo de investigación ilustra el potencial de eficiencia que las redes neuronales pueden alcanzar en la detección de fraude.

Por otro lado, basándonos en los estudios, se pudo obtener los siguientes resultados: la Red Neuronal Recurrente (RNN), alcanzó una precisión del 98.71%, la Red Neuronal Generativa Adversarial (GAN) para la misma tarea, logró una precisión notable del 97.1%. Asimismo, las Redes Neuronales de Memoria a Largo Plazo (LSTM) también fueron evaluadas, obteniendo una precisión del 96.68%. Por otro lado, las Redes Neuronales Artificiales (ANN) se utilizaron para la detección de anomalías, alcanzando una precisión del 96.35%, la Red Neuronal Convolucional (CNN) también se consideró, logrando una precisión del 95.69%. Otro estudio aplicó Redes Neuronales Autoencoder para la detección de fraude, obteniendo una precisión 85.65%. Estos resultados evidencian que las técnicas de redes

neuronales pueden ser altamente eficaces en la detección de fraudes financieros.

Tabla III. Nivel de eficiencia de las técnicas de redes neuronales

Artículos	**Red neuronal**	**Precisión**
Enfoque basado en redes neuronales para la detección de fraudes en Ethereum [13]	ANN	97.09%
Redes neuronales de gráficos adaptativos basadas en aprendizaje sensible a los costos para la detección de fraudes [14]	GAN	--
El diablo está en el conflicto: redes neuronales con gráficos de información desenredados para la detección de fraudes [15]	GAN	94.08%
Mejora de la eficiencia en la detección de anomalías: introducción de un algoritmo de optimización de enjambre de partículas multipoblacionales basado en búsqueda en cuadrícula basado en una red neuronal convolucional regional optimizada para soluciones robustas y escalables en datos de alta dimensión [16]	CNN	90%
Una red de atención gráfica semisupervisada para la detección de fraudes financieros [17]	GAN	90.07%
Comparación de técnicas de balanceo de datos para la detección de fraudes con tarjetas de crédito mediante redes neuronales [18]	ANN	90%
Detección de fraude financiero mediante redes neuronales híbridas convolucionales y recurrentes: un análisis de datos no estructurados en la banca [19]	RNN	99.02%
Método Análisis Envolvente de Datos y Redes Neuronales en la Evaluación y predicción de la Eficiencia Técnica de Pequeñas Empresas Exportadoras [20]	ANN	94.44%
Un estudio empírico del modelo de red neuronal MLP para problemas de predicción con salidas múltiples [21]	ANN	--
Detección de fraudes financieros bancarios mediante el ajuste de hiperparámetros de DL en un entorno de computación en la nube [22]	LSTM	--

Detección de anomalías en redes blockchain mediante aprendizaje no supervisado: una encuesta [23]	AE	--
Detección de fraudes impulsada por IA en transacciones financieras con redes neuronales gráficas y detección de anomalías [24]	GAN	95%
Marco de trabajo de redes neuronales basado en algoritmos genéticos para la detección de transacciones fraudulentas [25]	GAN	99.25%
Detección de rostros artificiales y engañosos mediante aprendizaje automático [26]	CNN	99.4%
Mejora de la detección de fraudes con tarjetas de crédito mediante análisis secuencial basado en LSTM con detención temprana [27]	LSTM	98%
Cómo proteger las finanzas digitales: aplicación del aprendizaje automático para el análisis de fraudes [28]	RNN	--
Enfoque algorítmico basado en aprendizaje automático para una mejor detección de anomalías en transacciones financieras [29]	ANN	--
Marco de trabajo de redes neuronales basado en algoritmos genéticos para la detección de transacciones fraudulentas [30]	GAN	99.25%
Enfoques de aprendizaje automático para la detección de fraudes con tarjetas de crédito: un análisis comparativo y la promesa de las redes neuronales convolucionales 1D [31]	CNN	--
Un modelo de memoria a corto plazo para la detección de fraudes con tarjetas de crédito [32]	RNN	99.6%
Mejorar la seguridad en los espacios públicos mediante redes generativas antagónicas (GAN) [33]	GAN	--
Mejora de la detección de fraudes financieros mediante un modelo de aprendizaje automático de conjunto ajustado por parámetros [34]	ANN	99.63%
Conjunto de redes neuronales gráficas para una mejor detección del fraude financiero [35]	GAN	--
Mejora de la seguridad en los pagos con billetera móvil: detección de fraudes basada en aprendizaje automático en las principales plataformas de billetera [36]	LSTM	93.8%
Detección de valores atípicos híbridos en conjuntos de datos de atención médica mediante DNN y una SVM de clase única [37]	AE	--

Un nuevo método para la detección de transacciones bancarias fraudulentas utilizando redes neuronales multicapa con tasa de aprendizaje adaptativa [38]	GNN	99%
Análisis del uso de redes de reconocimiento de patrones en la aplicación de redes eléctricas inteligentes [39]	ANN	99.99%
Un modelo de red neuronal convolucional para detectar URL ilegítimas [40]	CNN	94.31%
Calificaciones crediticias corporativas basadas en redes neuronales de grafos heterogéneos jerárquicos [41]	GAN	97%
Privacy-Preserving Behavioral Anomaly Detection in Dynamic Graphs for Card Transactions	GAN	95%
Una red generativa adversaria con autocodificador variacional mejorado con red neuronal convolucional para la detección de transacciones financieras fraudulentas	CNN	99.78%
Detección de fraudes en transacciones financieras mediante un enfoque de aprendizaje profundo: un estudio comparativo	ANN	97%
Marco de red neuronal basado en algoritmos genéticos para la detección de transacciones fraudulentas	GAN	99.25%
Detección de fraudes con tarjetas de crédito basada en SMOTE mediante redes neuronales convolucionales	CNN	99.96%
Predicción y análisis de la detección de fraudes en finanzas: un enfoque basado en el aprendizaje profundo y el aprendizaje automático	LSTM	98.25%
Combatir el fraude financiero digital mediante enfoques estratégicos de aprendizaje profundo	RNN	97.5%
Solución de detección de fraudes para transacciones monetarias con codificadores automáticos	AE	85%
Implementación estratégica de algoritmos de aprendizaje profundo para mitigar el fraude en las finanzas en línea	AE	86.3%

Considerando el nivel de precisión de las redes neuronales en cada documento evaluado en esta investigación, en la (Figura 5) se muestra la eficiencia de las redes neuronales más utilizadas para la detección de fraudes en transacciones financieras, dando una vista más general de los resultados de esta investigación.

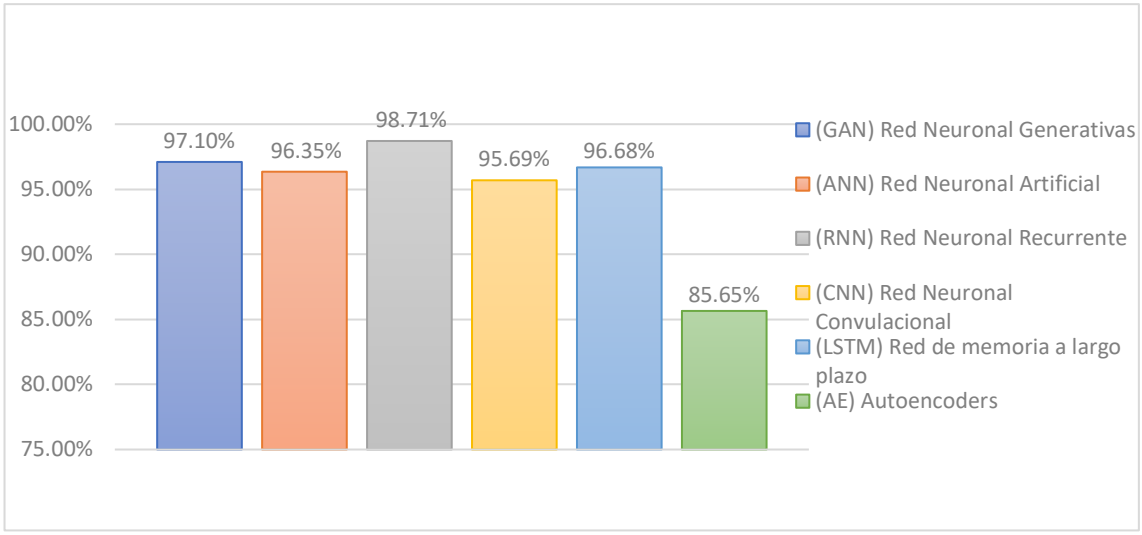

Figura 5. Eficiencias de las redes neuronales en la detección de fraude en transacciones financieras

Los resultados de esta investigación demuestran que las redes neuronales son altamente eficientes para detectar y reducir el riesgo de fraude en transacciones financieras. Donde, Ameijeiras S, Valdés S, & González D. (2021), sostienen que: La funcionalidad y eficiencia de cada red neuronal, incluyendo su capacidad para detectar fraudes financieros, dependen en gran medida de cómo está estructurada. La arquitectura de una red neuronal se refiere a la disposición de sus capas, el número de neuronas en cada capa, y las conexiones entre ellas. Un diseño adecuado es crucial, ya que una estructura bien optimizada permitirá a la red aprender y generalizar patrones en los datos de manera más efectiva. Por ejemplo, en la detección de fraudes, los modelos de red neuronal deben ser capaces de identificar patrones complejos y sutiles que pueden ser indicativos de actividades sospechosas. Si la red tiene una arquitectura demasiado simple, con pocas capas o neuronas, es probable que no capture la complejidad necesaria de los datos, resultando en un modelo que no es capaz de distinguir correctamente entre transacciones legítimas y fraudulentas [42].

Por otro lado, una red demasiado compleja puede llevar a problemas de sobreajuste, donde el modelo se adapta demasiado a los datos de entrenamiento, perdiendo su capacidad para generalizar a nuevas muestras de datos. Esto es especialmente problemático en el ámbito financiero, donde las condiciones y el comportamiento de los usuarios pueden cambiar con el tiempo. Una red estructurada de manera adecuada debe lograr un balance, permitiendo suficiente capacidad para aprender patrones relevantes sin caer en el sobreajuste.

En resumen, la estructura de una red neuronal es un determinante crítico de su funcionalidad y eficiencia en la detección de fraudes financieros. Una arquitectura bien diseñada permite a la red no solo aprender patrones complejos, sino también adaptarse a nuevas tendencias y comportamientos en los datos, lo que resulta esencial para el monitoreo efectivo de transacciones y la prevención de fraudes.

RQ3. ¿Cómo están evolucionando las técnicas de redes neuronales para abordar los desafíos y delitos emergentes en las instituciones financieras?

Las técnicas de redes neuronales están experimentando un progreso significativo en su aplicación para abordar los desafíos y delitos emergentes en el ámbito de las instituciones financieras. Esta evolución se evidencia a través de la combinación de la inteligencia artificial, aprendizaje profundo y análisis de datos, todas destinadas a reforzar la ciberseguridad y la integridad financiera. Las redes neuronales, siendo componentes esenciales de la inteligencia artificial, se utilizan con el objetivo de mejorar la detección y mitigación de amenazas financieras, como fraudes, lavado de dinero, manipulación del mercado y ataques cibernéticos.

En el estudio [43], se destaca el uso de modelos de aprendizaje profundo que pueden analizar patrones complejos y comportamientos anómalos en grandes conjuntos de datos financieros. Estos modelos no solo identifican transacciones fraudulentas de manera más efectiva, sino que también se adaptan continuamente a nuevas modalidades de amenazas, reflejando la naturaleza dinámica del panorama delictivo. Además, según [44], la integración de técnicas de procesamiento de lenguaje natural (PLN) y análisis de sentimientos se presenta como una estrategia innovadora para examinar las comunicaciones financieras en busca de indicios de actividades ilícitas. Este enfoque no solo aborda la detección de fraudes, sino que también se extiende a la identificación de información privilegiada y la evaluación de la confiabilidad de las fuentes de datos.

La aplicación de redes neuronales en la detección de fraude financiero constituye otra faceta crucial de esta evolución, donde la capacidad para analizar complejas relaciones entre transacciones y reconocer patrones asociados al fraude financiero, proporciona una herramienta invaluable para las instituciones financieras.

Podemos decir que un aspecto distintivo de esta evolución radica en la interconexión de datos provenientes de diversas fuentes, que incluyen transacciones financieras, comportamientos del cliente y datos externos. Esta integración multifacética potencia la precisión y la capacidad de contextualización en la detección de actividades sospechosas, ofreciendo una visión más completa del riesgo financiero, a continuación, en la (Tabla IV) se muestra el progreso de las redes neuronales para la detección de fraude en transacciones financieras a lo largo de los años.

Tabla VI. Evolución de las técnicas de redes neuronales

Primeras Aplicaciones (1990)	Durante esta década, las instituciones financieras comenzaron a explorar el uso de redes neuronales para detectar patrones de fraude en las transacciones. Estas primeras aplicaciones utilizaban perceptrones multicapa (MLP) y se enfocaban en detectar patrones inusuales en los datos transaccionales. Publicaciones y estudios comenzaron a surgir, explorando la viabilidad y efectividad de las redes neuronales para la detección de fraude.
Mejoras (2000)	La mejora en los algoritmos y métodos impulsaron a la adopción de redes neuronales para la detección de fraude, Las instituciones financieras comenzaron a implementar estos sistemas en sus operaciones diarias para mejorar la precisión en la detección de fraudes.
Evolución (2010)	Con el auge del aprendizaje profundo, se introdujeron redes neuronales más complejas y profundas en la detección de fraude. Las redes neuronales convolucionales (CNN) y las redes neuronales recurrentes (RNN) demostraron ser efectivas en la identificación de patrones de fraude más sofisticados.
Técnicas Avanzadas (2015-2024)	La integración de técnicas avanzadas como las redes generativas adversariales (GANs) y los autoencoders ha mejorado aún más la precisión y la capacidad de las redes neuronales para detectar fraudes. Estas técnicas permiten generar datos sintéticos y reconstruir patrones normales para identificar anomalías. La implementación de soluciones de inteligencia artificial en tiempo real ha permitido a las instituciones financieras detectar y prevenir fraudes de manera más efectiva y rápida.

4. CONCLUSIONES:

Los hallazgos de este estudio subrayan el papel crucial que desempeñan las redes neuronales en la detección de fraudes en transacciones financieras, y resaltan la importancia de implementar

tecnologías avanzadas en la protección de sistemas financieros. Con el constante avance de la tecnología, la inteligencia artificial y los métodos fraudulentos, la identificación de patrones de comportamiento inusual se vuelve esencial para reducir el riesgo de fraude en las transacciones financieras.

Además cabe destacar que considerando los resultados obtenidos en la pregunta RQ1 y RQ2, donde en la primera se obtiene que las redes GAN son las más utilizadas no esta de la mano con los resultados de la segunda pregunta donde se evalúa el nivel de

La obtención de resultados satisfactorios en la detección de fraudes en transacciones financieras mediante el uso de redes neuronales representa un avance significativo y prometedor en el ámbito de la seguridad financiera. El éxito de las redes neuronales en la detección de fraudes se debe en gran parte a su capacidad para procesar grandes volúmenes de datos y aprender de ellos de manera continua, proporcionando un análisis del rendimiento de diferentes modelos de redes neuronales. Este estudio ayuda a profundizar en la comprensión del impacto y la eficacia de las redes neuronales en la detección de fraudes financieros.

Para investigaciones futuras, sería recomendable evaluar el desempeño de las redes neuronales utilizando datos en línea para medir su capacidad de detección en tiempo real lo que permitiría medir no solo su capacidad de detección de fraude, sino también su velocidad y adaptabilidad ante amenazas emergentes. El uso de datos en tiempo real proporcionaría una comprensión más profunda de cómo estos modelos responden a patrones cambiantes y nuevas metodologías de fraude, que a menudo evolucionan rápidamente.

Además, este estudio evidencia la necesidad de seguir avanzando en el desarrollo de modelos de redes neuronales que no solo se adapten a las cambiantes estrategias de los delincuentes, sino que también integren nuevas tecnologías y enfoques. Esto es crucial para garantizar que las redes

neuronales sigan siendo eficaces en la detección y prevención de fraudes.

En resumen, la investigación pone de manifiesto no solo el potencial de las redes neuronales en la detección de fraudes financieros, sino también la importancia de una vigilancia continua y de la innovación constante para enfrentar de manera efectiva las amenazas en un panorama financiero cada vez más complejo y dinámico. La inversión en estas tecnologías y en la formación de profesionales capacitados para su desarrollo y aplicación será clave para el fortalecimiento de la seguridad financiera global.

5. REFERENCIAS BIBLIOGRAFICAS:

[1] Chuquiana, A., & Maoli, E. (2023) «Análisis del ataque del modelo Phishing en los sistemas informáticos y bancarios», Babahoyo, Ecuador. Universidad Técnica de Babahoyo, págs. 1-16. [En línea]. Disponible en: http://dspace.utb.edu.ec/handle/49000/14773

[2] Castiblanco. C & Jorge. L. (2024) «La importancia de la gestión en la prevención del fraude interno en las entidades financieras.» Bogotá, Colombia. Repositorio Unimilitar, págs. 1-9. Accedido: 22 de julio de 2024. [En línea]. Disponible en: https://repository.unimilitar.edu.co/handle/10654/35987

[3] Vargas, O., (2022) «Detección de anomalías en procesos de gestión sanitaria usando métodos de analítica de procesos». Bogotá, Colombia, Universidad de los Andes, págs. 1-3. [En línea]. Disponible en: https://repositorio.uniandes.edu.co/flip/?pdf=https://repositorio.uniandes.edu.co/bitstreams/76ce883b-ec57-49f7-b492-cc619540e9e9/download

[4] Torres, H. (2022), «Fraudes bancarios: algunos fraudes financieros y riesgos asociados», Medellín, Colombia. Universidad de Antioquía, págs. 1-12 [En línea]. Disponible en: https://digitk.areandina.edu.co/handle/areandina/4755

[5] Londoño. L., Carmona. M, (2021) «Modelos de machine learning para la detección de fraude financiero», Medellín, Colombia. Universidad de Antioquía, págs. 1-10 [En línea]. Disponible en: https://bibliotecadigital.udea.edu.co/handle/10495/20164

[6] Pérez, G., (2021) «Detección de transacciones fraudulentas en tarjetas de crédito mediante el uso de modelos de Machine Learning», Bogotá, Colombia, Universidad de los Andes, págs. 1-6. [En línea]. Disponible en: https://repositorio.uniandes.edu.co/server/api/core/bitstreams/f1f6f0ea-f5e4-4e09-9c3d-393c288ac42d/content

[7] Ramírez, A., Jenkins, M., Martínez, A., Quesada, C., (2020) «Usodetcnicasdemineradedatosyaprendizajeautomticoparadeteccindefraudesenestadosfinancieros», San Pedro, Costa Rica. Universidad de Costa Rica, págs. 97-109 [En línea]. Disponible en: https://www.mendeley.com/reference-manager/reader-v2/ed2e9e71-9b6b-39b5-b757-6a034ffd81a3/42ec9c60-f88e-98db-38b0-1d5c148eae1e

[8] Quirumbay, D., Castillo, C., coronel, I., (2022) «Una revisión del aprendizaje profundo aplicado a la ciberseguridad», Santa Elena, Ecuador. Revista Científica y Tecnológica UPSE (RCTU), [Online]. Disponible en: https://incyt.upse.edu.ec/ciencia/revistas/index.php/rctu/article/download/671/556?inline=1

[9] Muñoz, M., De Chile, (2019) «UNIVERSIDAD DE CHILE FACULTAD DE

CIENCIAS FÍSICAS Y MATEMÁTICAS DEPARTAMENTO DE INGENIRÍA CIVIL PRONÓSTICO DE CRECIDAS EN TIEMPO REAL USANDO REDES NEURONALES RECURRENTES MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL MILENA MUÑOZ BONACIC PROFESOR GUÍA: XIMENA VARGAS MESA», Santiago de Chile, Chile. RepositoriosUchile [En línea]. Disponible en: https://repositorio.uchile.cl/bitstream/handle/2250/104857/Prono%cc%81stico-de-crecidas-en-tiempo-real-usando-redes-neuronales-recurrentes.pdf?sequence=3&isAllowed=y

[10] Ameijeiras. D., Valdés. O., & González. H. (2021). «Algoritmos de detección de anomalías con redes profundas. Revisión para detección de fraudes bancarios». La Habana, Cuba. Revista Cubana de Ciencias Informáticas, [Online]. Disponible en: http://scielo.sld.cu/scielo.php?pid=S2227-18992021000500244&script=sci_arttext&tlng=en

[11] Edu, P., (2024) «Propuesta de modelo predictivo para la detección de fraude en mensajes de texto mediante el uso de Redes Neuronales Recurrentes», Lima, Perú. Repositorios institucionales Esan, [En línea]. Disponible en: https://repositorio.esan.edu.pe/items/d89b8826-b5f1-4b93-85e3-bb6b7daa6a30

[12] Cho. k., (2018) «Learning phrase representations using RNN encoder-decoder for statistical machine translation», Doha, Qatar. Conference on Empirical Methods in Natural Language Processing, Proceedings of the Conference, págs. 1724-1732 [Online]. Disponible en: https://aclanthology.org/D14-1179

[13] Dahiya. M, Mishra. N, Singh. R, y Pavitra, (2023) «Neural network-based approach for Ethereum fraud detection», Londres, Reino Unido, 2023, págs. 1-4, doi: 10.1109/ICIEM59379.2023.10166745.

[14] Yan. Q., (2024) «An Adaptive Graph Neural Networks Based on Cost-sensitive Learning for Fraud Detection», Chongqing, China. Publicado en: 2024 7º Simposio Internacional sobre Sistemas Autónomos (ISAS), págs 1-6, [Online]. Disponible en: https://ieeexplore.ieee.org/document/10552392

[15] Li. Z, Chen. D, Liu. Q, y Wu. S, (2022) «The Devil is in the Conflict: Disentangled Information Graph Neural Networks for Fraud Detection» Orlando, Florida, EE. UU. Proceedings - IEEE International Conference on Data Mining, ICDM, vol. 2022-November, [Online]. Disponible en: https://ieeexplore.ieee.org/document/10027689

[16] Nalini. M, Yamini. B, Fernandez. M. y Uma P, (2024) «Mejora de la eficiencia en la detección de anomalías: introducción de un algoritmo de optimización de enjambre de partículas multipoblacionales basado en búsqueda en cuadrícula basado en una red neuronal convolucional regional optimizada para soluciones robustas y escalables en datos de alta dimensión», Chennai, India. Departamento de Ciencias Informáticas e Ingeniería. [Online]. Disponible en: DOI: 10.1016/j.eswa.2024.125179

[17] Wang. D, (2019) «A semi-supervised graph attentive network for financial fraud detection», Pekín, China. Proceedings - IEEE International Conference on Data Mining, ICDM. [Online]. Disponible en: https://ieeexplore.ieee.org/document/8970829

[18] Uttam A., y Sharma. G, (2021) «A Comparison of Data Balancing Techniques for Credit Card Fraud Detection using Neural Network», Palladam, India. Proceedings of the 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2021[Online]. Disponible en: https://ieeexplore.ieee.org/document/9640911

[19] Banu S., Gongada T., Santosh. K, Chowdhary. H, Sabareesh. R, y Muthuperumal. S, (2024) «Financial Fraud Detection Using Hybrid Convolutional and Recurrent Neural Networks: An Analysis of Unstructured Data in Banking», Melmaruvathur, India. Proceedings of the 2024 10th International Conference on Communication and Signal Processing, ICCSP 2024, [Online]. Disponible en: https://ieeexplore.ieee.org/document/10543545

[20] Fontalvo. T, Hoz. L, y E. De, (2018) «Método Análisis Envolvente de Datos y Redes Neuronales en la Evaluación y Predicción de la Eficiencia Técnica de Pequeñas Empresas Exportadoras Data Envelopment Analysis Method and Neural Networks in the Evaluation and Prediction of the Technical Efficiency of Small Exporting Companies»,

Cartagena, Colombia. Información Tecnológica, [Online]. Disponible en: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642018000600267&lng=en&nrm=iso&tlng=en
[21] Camejo. J, Gonzalez. H., y Morell. C, (2020) «Un estudio empírico del modelo de red neuronal MLP para problemas de predicción con salidas múltiples», La Habana, Cuba. Serie Científica de la Universidad de las Ciencias Informáticas, ISSN-e 2306-2495, Vol. 13, Nº. 6, 2020, págs. 1-14, vol. 13, n.º 6, pp. 1-14, 2020, Accedido: 28 de julio de 2024. [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8590275&info=resumen&idioma=ENG
[22] Upreti. K, Vats. P, Srinivasan. A, Daya. K., Mahaveerakannan. R, y Charles. G, «Detección de fraudes financieros bancarios mediante el ajuste de hiperparámetros de DL en un entorno de computación en la nube», Nueva Delhi, India. Revista Internacional de Sistemas de Información Cooperativa, [Online]. Disponible en: DOI: 10.1142/S0218843023500247
[23] Cholevas. C, Angeli. E, Sereti. Z, Mavrikos. E, y Tsekouras. G. E, (2024) «Detección de anomalías en redes blockchain mediante aprendizaje no supervisado: una encuesta», Mitilene, Grecia. Departamento de Tecnología Cultural y Comunicación, Universidad del Egeo, [Online]. Disponible en: DOI: 10.3390/a17050201
[24] Thilagavathi. M, Saranyadevi. R, Vijayakumar. N, Selvi. K, Anitha. L, y Sudharson. K, (2024) «Detección de fraudes impulsada por IA en transacciones financieras con redes neuronales gráficas y detección de anomalías», Chennai, India. Actas de la Conferencia internacional de 2024 sobre ciencia, tecnología, ingeniería y gestión, ICSTEM 2024, [Online]. Disponible en: DOI: 10.1109/ICSTEM61137.2024.10560838
[25] Jahan. I y Kumar. M, (2023) «Marco de trabajo de redes neuronales basado en algoritmos genéticos para la detección de transacciones fraudulentas», Greater Noida, Uttar Pradesh, India. Actas de la 4.ª Conferencia internacional IEEE 2023 sobre informática, comunicación y sistemas inteligentes, ICCCIS 2023, [Online]. Disponible en: DOI: 10.1109/ICCCIS60361.2023.10425407
[26] Nachiappan. B, Rajkumar. N, Viji. C, y Mohanraj. A, «Detección de rostros artificiales y engañosos mediante aprendizaje automático [Detección de rostros artificiales y engañosos mediante aprendizaje automático», Karnataka, Bangalore, India. Salud, Ciencia y Tecnología - Serie de Conferencias, vol. 3, [Online]. Disponible en: DOI: 10.56294/sctconf2024611
[27] Jhansi. S, Balasubadra. K, Skandarsini. R., y Lakshmi. T, (2024) «Mejora de la detección de fraudes con tarjetas de crédito mediante análisis secuencial basado en LSTM con detención temprana», Thiruvallur, India. Actas de la 2.ª Conferencia internacional IEEE sobre redes y comunicaciones 2024, ICNWC 2024, [Online]. Disponible en: DOI: 10.1109/ICNWC60771.2024.10537550
[28] Al. M, Aburub. F, Matar. N, Nofal. M. I, Sowan. B, y Fasha. M, (2024) «Cómo proteger las finanzas digitales: aplicación del aprendizaje automático para el análisis de fraudes», Ammán, Jordania. 2ª Conferencia Internacional sobre Ciberresiliencia, ICCR 2024, [Online]. Disponible en: DOI: 10.1109/ICCR61006.2024.10533140
[29] Sivakumar, Mariyappan, y Prakash. P., «Enfoque algorítmico basado en aprendizaje automático para una mejor detección de anomalías en transacciones financieras», Bengaluru, India. Apuntes de la asignatura de Ingeniería de Datos y Tecnologías de la Comunicación, vol. 93, págs.779-790, [Online]. Disponible en: DOI: 10.1007/978-981-16-6605-6_59
[30] Jahan. I y Kumar. M, (2023) «Genetic Algorithm Based Neural Network Framework for Fraudulent Transaction Detection», Greater Noida, India. Proceedings - 4th IEEE 2023 International Conference on Computing, Communication, and Intelligent Systems, ICCCIS 2023, págs. 631-635, [Online]. Dispnible en: https://ieeexplore.ieee.org/document/10425407
[31] Paulraj. B, (2024) «Machine Learning Approaches for Credit Card Fraud

Detection: A Comparative Analysis and the Promise of 1D Convolutional Neural Networks», Honolulu, HI, EE. UU. Proceedings - 2024 7th International Conference on Information and Computer Technologies, ICICT 2024, págs. 82-92, [Online]. Disponible en: https://ieeexplore.ieee.org/document/10541645
[32] Owolafe. O, Ogunrinde. O. B, y Thompson. A. F. B, «Un modelo de memoria a corto plazo para la detección de fraudes con tarjetas de crédito», Akure, Nigeria. Estudios en Inteligencia Computacional, vol. 972, Springer Science and Business Media Deutschland GmbH, págs. 369-391. [Online]. Disponible en: DOI: 10.1007/978-3-030-72236-4_15
[33] Ponnusamy. S, Antari. J, Bhaladhare. P, Potgantwar. A, y Kalyanaraman. S, (2024) «Mejorar la seguridad en los espacios públicos mediante redes generativas antagónicas (GAN)», Nashik, India Mejorar la seguridad en los espacios públicos mediante redes generativas antagónicas (GAN), págs. 1-409, [Online]. Disponible en: https://www.igi-global.com/book/enhancing-security-public-spaces-through/336531
[34] Atassi. R, Zikriyoev. A, Turayev. N, y Botırovna. S., (2022) «Mejora de la detección de fraudes financieros mediante un modelo de aprendizaje automático de conjunto ajustado por parámetros», United Arab Emirates, Uzbekistan. Revista de Ciberseguridad y Gestión de la Información, vol. 13, n.º 2, págs. 66-74, [Online]. Disponible en: DOI: 10.54216/JCIM.130205
[35] Hiremath. A., Arya. A, Sriranga. L, Reddy K y Nikhil. M, (2024) «Ensemble of Graph Neural Networks for Enhanced Financial Fraud Detection», Pune, India. págs. 1-8, jun. 2024, [Online]. Disponible en: https://ieeexplore.ieee.org/document/10543898
[36] Abdirahman. A., Hashi. A., Dahir. U., Elmi. M., y Rodriguez. O., «Mejora de la seguridad en los pagos con billetera móvil: detección de fraudes basada en aprendizaje automático en las principales plataformas de billetera», Thiruvallur, India. Revista internacional SSRG de ingeniería electrónica y de comunicaciones, vol. 11, n.º 3, págs. 96-105, [Online]. Disponible en: DOI: 10.1109/ICNWC60771.2024.10537550
[37] Thomas. R y Judith. J. E, (2020) «Detección de valores atípicos híbridos en conjuntos de datos de atención médica mediante DNN y una SVM de clase única», Kumaracoil, India. Actas de la 4ª Conferencia internacional sobre electrónica, comunicaciones y tecnología aeroespacial, ICECA 2020, págs. 1293-1298, [Online]. Disponible en: DOI: 10.1109/ICECA49313.2020.9297401
[38] Faridpour. M y Moradi. A, «Un nuevo método para la detección de transacciones bancarias fraudulentas utilizando redes neuronales multicapa con tasa de aprendizaje adaptativa», Revista internacional de análisis no lineal y aplicaciones, vol. 11, n.º 2, pp. 437-445, doi: 10.22075/ijnaa.2020.4576.
[39] Talledo R., y Álava. L., «Análisis del uso de redes de reconocimiento de patrones en la aplicación de redes eléctricas inteligentes [Análisis del uso de redes eléctricas inteligentes][Análisis del empleo de redes de reconocimiento de patrones en la aplicación de redes eléctricas inteligentes]», Portoviejo, Ecuador. Sapienza, vol. 3, n.º 2, págs. 816-825, DOI: 10.51798/sijisv3i2.408
[40] Al-Milli. N y Hammo. B., (2020) «Un modelo de red neuronal convolucional para detectar URL ilegítimas», Amam Jordania. 2020 11ª Conferencia Internacional sobre Sistemas de Información y Comunicación, ICICS 2020, págs. 220-225, [Online]. Disponible en: DOI: 10.1109/ICICS49469.2020.239536
[41] Feng. B., Cheng. X, Xu. H., y Xue. W., «Calificaciones crediticias corporativas basadas en redes neuronales de grafos heterogéneos jerárquicos», Beijing, China. Investigación en inteligencia de máquinas, vol. 21, n.º 2, págs. 257-271, [Online]. Disponible en: DOI: 10.1007/s11633-023-1425-9
[42] Ameijeiras S, Valdés S, & González D. (2021). «Algoritmos de detección de anomalías con redes profundas. Revisión para detección de fraudes bancarios.» La Habana, Cuba. Revista Cubana de Ciencias Informáticas, 15(4), 244–264. [Online]. Disponible en: http://scielo.sld.cu/scielo.php?pid=S2227-18992021000500244&script=sci_arttext&tlng=en

[43] Lissette. J y Moran. Z, «La inteligencia artificial en la detección de intrusiones en entornos de redes definidas por software (SDN).», Babahoyo, Ecuador. Págs. 1-55. 2023, Accedido: 28 de julio de 2024. [En línea]. Disponible en: http://dspace.utb.edu.ec/handle/49000/15119
[44] VR Saddi, B. Gnanapa, S. Boddu y J. Logeshwaran, "El papel del procesamiento del lenguaje natural en la detección del fraude en seguros", 2023 4th International Conference on Communication, Computing and Industry 6.0 (C216), Bangalore, India, 2023, págs. 1-6, doi: 10.1109/C2I659362.2023.10430658.
[45] Ranganatha. H, Syed Mustafa. A (2024) « Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3d Quasi-Recurrent Neural network and blockchain technologies » Karnataka, Belagavi, India. [Online]. disponible en: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85203871141&doi=10.1016%2fj.eswa.2024.125179&partnerID=40&md5
[46] Damoun, F., Seba, H., State, R. (2024) «Privacy-Preserving Behavioral Anomaly Detection in Dynamic Graphs for Card Transactions» Villeurbanne, Francia. pp. 286-301. [Online]. Disponible en: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85211250721&doi=10.1007%2f978-981-96-0576-7_22&partnerID=40&m
[47] Lin, J., Guo, X., Zhu, Y., Mitchell, S., Altman, E., Shun, J. «FraudGT: A Simple, Effective, and Efficient Graph Transformer for Financial Fraud Detection» (2024) ICAIF 2024 - 5th ACM International Conference on AI in Finance, pp. 292-300. 1) https://www.scopus.com/inward/record.uri?eid=2-s2.0-85214894401&doi=10.1145%2f3677052.3698648&partnerID=40&md5=7DOI: 10.1145/3677052.3698648
[48] Gudivaka, B. Almusawi, M. Priyanka, M. Dhanda, M. y Thanjaivadivel, M. «Una red generativa adversaria con autocodificador variacional mejorado con red neuronal convolucional para la detección de transacciones financieras fraudulentas», Segunda Conferencia Internacional sobre Ciencia de Datos y Sistemas de Información (ICDSIS) de 2024, Hassan, India, 2024, págs. 1-4, doi: 10.1109/ICDSIS61070.2024.10594271.
[49] Shanbhog. N, Totad. K, Hanchinal. A y Bidargaddi. A, «Detección de fraudes en transacciones financieras mediante un enfoque de aprendizaje profundo: un estudio comparativo», 2024 5th International Conference for Emerging Technology (INCET), Belgaum, India, 2024, págs. 1-7, doi: 10.1109/INCET61516.2024.10593486.
[50] Jahan. I y Kumar. M, «Marco de red neuronal basado en algoritmos genéticos para la detección de transacciones fraudulentas», Conferencia internacional sobre informática, comunicación y sistemas inteligentes (ICCCIS) de 2023, Gran Noida, India, 2023, págs. 631-635, doi: 10.1109/ICCCIS60361.2023.10425407.
[51] Yousuf. M, Kabir. T, Raka. N, Siddikha. S, Rahman. M y Ferdaus. J, «Detección de fraudes con tarjetas de crédito basada en SMOTE mediante redes neuronales convolucionales», 25.ª Conferencia internacional sobre informática y tecnología de la información (ICCIT) de 2022, Cox's Bazar, Bangladesh, 2022, págs. 55-60, doi: 10.1109/ICCIT57492.2022.10054727.
[52] Sheth. A, Nair. A, Rai. A y Sawant. R, «Predicción y análisis de la detección de fraudes en finanzas: un enfoque basado en el aprendizaje profundo y el aprendizaje automático», 2024 4th International Conference on Intelligent Technologies (CONIT), Bangalore, India, 2024, págs. 1-6, doi: 10.1109/CONIT61985.2024.10626214.
[53] Sharma. R y Sharma. A, «Combatir el fraude financiero digital mediante enfoques estratégicos de aprendizaje profundo», 2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS) , Coimbatore, India, 2024, págs. 824-828, doi: 10.1109/ICSCSS60660.2024.10625249.
[54] Chandradeva. L, Jayasooriya. I y Aponso. A, «Solución de detección de fraudes para transacciones monetarias con codificadores automáticos», Conferencia Nacional de Tecnología de la Información (NITC) de 2019, Colombo, Sri Lanka, 2019, págs. 31-34, doi: 10.1109/NITC48475.2019.9114519.
[55] Sharma. R and Gupta. S, «Strategic Deployment of Deep Learning Algorithms to

Mitigate Fraud in Online Finance», 2024 7th International Conference on Circuit Power and Computing Technologies (ICCPCT), Kollam, India, 2024, pp. 1007-1011, doi: 10.1109/ICCPCT61902.2024.10673115.