Importancia del machine learning en la seguridad de la información dentro del ámbito financiero

Importance of machine learning in information security within the financial field

Maricielo Estefany Caciano Arroyo, Antony Fernando Vasquez Cabrera, Alberto Carlos Mendoza de los Santos

Universidad Nacional de Trujillo, Trujillo, Perú

Recibido: 14/02/2023 Revisado: 11/04/2023 Aceptado: 25/05/2023 Publicado: 31/07/2023

Resumen

En la actualidad, el sector financiero está en constante evolución gracias a la aplicación de la inteligencia artificial, esta herramienta ha demostrado su gran poder en la capacidad de detectar y prevenir fraudes financieros. Sin embargo, estos delitos continúan siendo un riesgo para la protección de los datos sobre las instituciones financieras, lo que ha llevado a la implementación del Machine Learning como una medida eficaz para erradicar estas acciones ilegales.

Se ha realizado una revisión sistemática con el propósito de evaluar la relevancia del aprendizaje automático en la protección de la información en el ámbito financiero. Durante este proceso, se han analizado exhaustivamente los estudios publicados en el período comprendido desde el 2021 hasta el 2023.

Según los resultados obtenidos, la gran mayoría de los resultados revelan que los sistemas económicos emplean diferentes métodos de Machine Learning que contribuyen de forma efectiva a prevenir los fraudes y otras amenazas que afectan al sector. En este sentido, se pone de manifiesto la gran relevancia que tiene esta tecnología para avalar la seguridad de la información financiera.

Palabras Claves:

Aprendizaje Automático, Seguridad de la información, Sector financiero, Inteligencia Artificial.

Abstract

Currently, the financial sector is constantly evolving thanks to the application of artificial intelligence, this tool has demonstrated its great power in the ability to detect and predict financial fraud. However, these crimes continue to be a risk for the protection of data on financial institutions, which has led to the implementation of Machine Learning as an effective measure to eradicate these illegal actions.

A systematic review has been conducted with the purpose of evaluating the relevance of Machine Learning in the protection of information in the financial field. During this process, studies published in the period from 2021 to 2023 have been thoroughly analyzed.

The findings obtained show that most of the results reveal that economic systems employ different Machine Learning methods that effectively contribute to prevent fraud and other threats affecting the sector. In this sense, the great relevance of this technology in guaranteeing the security of financial information becomes evident.

Keywords:

Machine Learning, Information security, financial sector, Artificial Intelligence.

Introducción

En la actualidad, la inteligencia artificial ha ganado una enorme importancia y se ha transformado en una herramienta esencial y ampliamente utilizada en las entidades financieras. Para entender mejor la definición de inteligencia artificial se presenta el siguiente concepto: La finalidad de la inteligencia artificial es conseguir que los ordenadores realicen tareas similares a las que la mente humana puede llevar a cabo para poder crear sistemas automáticos que faciliten la ejecución de dichas tareas (Boden, 2017).

Una vez que se ha presentado su definición, se puede afirmar que el uso de la inteligencia artificial es esencial para el progreso del ámbito financiero. Por lo tanto, las entidades financieras están adoptando cada vez más la inteligencia artificial con el propósito de fortalecer la seguridad, disminuir los gastos y aumentar la eficacia en sus operaciones.

La inteligencia artificial tiene múltiples aplicaciones significativas, y una de las más destacadas en la gestión de la información es la seguridad. La IA puede ayudar a proteger la información utilizando tecnologías como el aprendizaje automático (Machine Learning), que según Hinestroza Ramírez (2018) menciona que esta herramienta tiene como propósito principal optimizar el manejo y evaluación de la información. Con el fin de realizar predicciones futuras, ya sea mediante la ejecución de nuevos sistemas o la optimización de los existentes. Es por ello

que puede mejorar la capacidad de las entidades bancarias para detectar y responder rápidamente a incidentes de seguridad.

Según Calderón (2015), en una organización, se consigue la protección de la información por medio de la aplicación de múltiples medidas técnicas, organizativas y legales que aseguran que el sistema de información mantenga su confidencialidad, integridad y disponibilidad.

Cuando nos referimos a esta definición, podemos concluir que se refiere a un conjunto de tácticas y medidas aplicadas para controlar y salvaguardar los datos administrados en una compañía, con el propósito de asegurar que esa información no salga del sistema establecido por la organización.

En un sistema de información financiera este aspecto es especialmente crítico, ya que la información confidencial y personal de los clientes debe ser protegida de forma rigurosa para evitar su uso fraudulento y garantizar la confianza de los clientes en la institución financiera.

En resumen, la inteligencia artificial se ha transformado en un instrumento fundamental para el sector financiero, como resultado, se logra fortalecer la protección de los datos y optimizar la eficacia en las operaciones de las instituciones financieras. En este sentido, es importante que las instituciones financieras comprendan el potencial de la inteligencia artificial y lo utilicen de manera efectiva con el objetivo de cumplir con las exigencias de los clientes y permanecer competitivas en un contexto en constante evolución y digitalizado.

El motivo de esta investigación es exponer las distintas tecnologías de la inteligencia artificial utilizadas actualmente en la protección de la información en el ámbito de las instituciones financieras. A raíz de lo expuesto previamente, se ha planteado la siguiente interrogante de exploración: ¿Cuál es la relevancia de la aplicación de la tecnología de Machine Learning en el ámbito financiero para avalar la seguridad de la información?

Con el fin de abordar esta pregunta, se realizó una exhaustiva investigación en destacadas bases de datos que contienen publicaciones relacionadas con el tema en cuestión y que son relevantes para lograr el objetivo establecido. Se utilizó el enfoque PRISMA para seleccionar y evaluar los resultados obtenidos de las investigaciones seleccionadas. Por último, se exponen las conclusiones breves que resaltan la importancia del Machine Learning en el campo de las finanzas.

Materiales y Métodos

Tipo de Estudio

Se empleó la metodología PRISMA en la ejecución de este análisis exhaustivo. La pregunta de investigación que se planteó para poder ser contestada de manera objetiva es: ¿Cuál es la

relevancia de la aplicación de la tecnología de Machine Learning en el ámbito financiero para avalar la seguridad de la información?

Fundamentación de la Metodología

Antes de adentrarnos en la fundamentación de la metodología PRISMA, se necesita explicar primero qué es una revisión sistemática. Según Moreno et al. (2022), nos menciona que son síntesis organizadas y estructuradas de la información disponible, que tienen como objetivo responder una pregunta específica. Estas evaluaciones se fundamentan en una variedad de fuentes de datos y documentos, y, por lo tanto, representan el grado más alto de sustento dentro de la estructura jerárquica de evidencias.

Para elaborar una revisión sistemática, se requiere seguir una secuencia de pasos organizados y estructurados. Estos pasos se ven reflejados en el tipo de metodología que la revisión sistemática utilice. En esta situación particular, se ha empleado la metodología PRISMA, que según Urrútia y Bonfill (2010), proporciona recomendaciones para incrementar la calidad y exactitud de los informes de revisiones sistemáticas y metaanálisis. A partir de su fecha de publicación en 2009, la declaración PRISMA ha sido ampliamente utilizada por autores e investigadores de todo el mundo.

Teniendo en cuenta esta definición de la metodología PRISMA, se observa que es importante utilizar en una revisión sistemática la ayuda de esta metodología. Para comenzar a desarrollar este método, se seguirán los siguientes pasos mencionados por Arnau y Sala (2020): el proceso consiste en crear un plan de búsqueda, reconocer y elegir los materiales relevantes, y luego registrar y organizar los resultados obtenidos de manera similar al análisis y la comprensión de los datos seleccionados.

Estrategia de búsqueda

Para poder encontrar la información que se requería sobre el tema de investigación, se emplearon ciertas palabras claves utilizados en el sistema de búsqueda que cubre todas las bases de datos, estos términos fueron: “financial”, “security”, “Machine Learning”, “security information”, “intelligence artificial”, “seguridad financiera”, “aprendizaje automático”.

Se crearon pautas para seleccionar las fuentes de información requeridas con el objetivo de realizar la investigación con datos fidedignos y pertinentes. Entre ellos se encuentran REDALYC, SCOPUS, SCIENCE DIRECT, RESEARCHGATE, WORLDWIDE SCIENCE, SEMANTIC SCHOLAR Y GOOGLE ACADÉMICO, los cuales fueron utilizados para recopilar información y obtener resultados más precisos y actualizados (Figura 1). La inclusión de estas fuentes garantiza la calidad y pertinencia de los datos recopilados y analizados en la investigación.

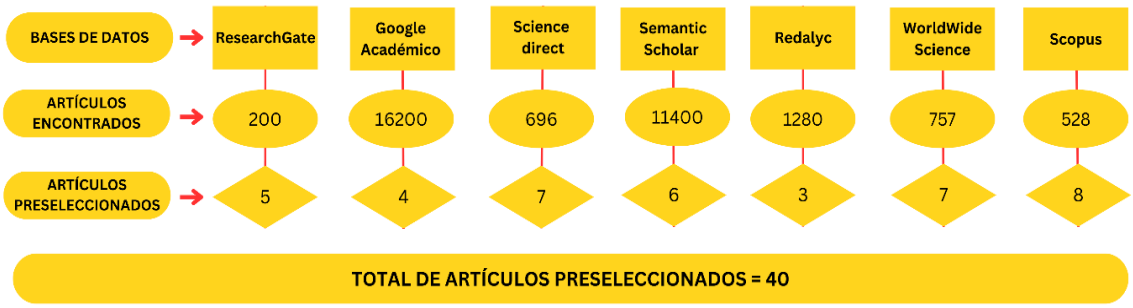

Figura 1. Exploración en bancos de datos y filtrado preliminar de artículos.

Criterios de inclusión y de exclusión

En cuanto a la incorporación de los documentos en el estudio, se tuvieron en cuenta los artículos de investigación escritos en ambos idiomas, en ambos idiomas, inglés y español y se emplearon diferentes bases de datos como para ampliar la indagación y obtener una muestra representativa.

Con respecto a los años de investigación, se establecieron las fechas comprendidas desde el 2021 hasta el 2023, con el fin de obtener documentos actualizados y relevantes para la investigación en cuestión.

Además, se identificaron los tipos de documentos académicos que se incluirían en el análisis, entre ellos se encuentran los artículos, los artículos de conferencias y los artículos de revisión. Es importante destacar que, para garantizar la disponibilidad de los documentos, se estableció como criterio de inclusión que los mismos estén accesibles en línea.

Por otro lado, para el criterio de exclusión se descartaron aquellas publicaciones que abordan temas irrelevantes para la investigación, tales como artículos de temas médicos y químicos. De esta manera, se garantiza que la selección de documentos sea pertinente y esté enfocada en los objetivos de la investigación, además, esto ayudará a mejorar la calidad y confiabilidad de los resultados alcanzados. (Figura 2).

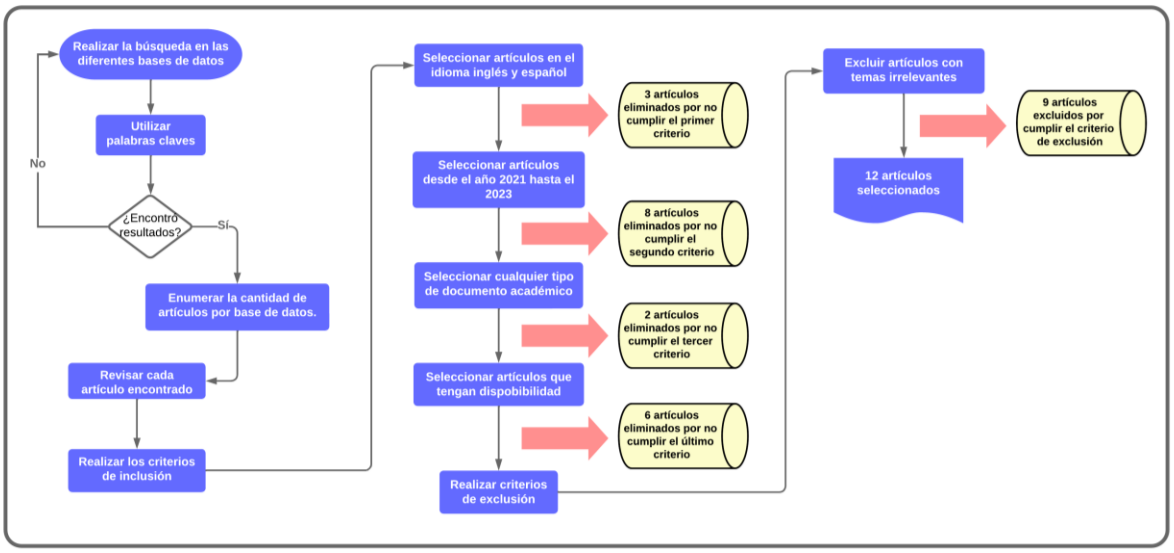

Figura 2. Diagrama de flujo que detalla los criterios para incluir o excluir a determinados elementos.

Resultados y Discusión

Para la investigación y recopilación de datos tomamos en cuenta los 40 artículos preseleccionados, luego elegimos aquellos que satisfacían los requisitos de inclusión y exclusión que habíamos definido previamente, de esta manera se muestra en la (Tabla 1) los aportes principales de cada artículo.

Tabla 1

Enumeración de artículos que satisfacen los criterios expuestos anteriormente.

N°	Autor(es)	Título	Año	País	Principales Aportes
1	G Kasi Reddy, P. Naresh, M. Bhargavi, Pannangi Rajyalakshmi, Ch V Raghavendran y B. Narsimha	Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application	2022	India	Un resultado experimental muestra que las firmas financieras pueden detectar fraudes e identificar transacciones genuinas en tiempo real utilizando la herramienta de aprendizaje automático abierto de software de Feedzai's con mayor precisión.
2	Vedant Shah	How effective is Machine Learning at detecting financial fraud using mobile transaction metadata?	2022	India	El desarrollo y análisis de un modelo de aprendizaje automático utilizado para detectar el fraude financiero en las transacciones de dinero móvil. El objetivo de este documento es discutir qué tan efectivo puede ser un modelo de

					aprendizaje automático para detectar fraudes en transacciones automáticas.
3	Bobyk Andrzej, Księżopolski Bogdan, Srokosz Michał y Wydra Michal	Machine-Learning-Based Scoring System for Antifraud CISIRTs in Banking Environment	2023	Polonia	Diseñaron un sistema de calificación basado en el aprendizaje automático que brinda advertencias tempranas contra el fraude financiero.
4	Nhien-An Le-Khac, Aditya Kuppa y Jack N.	Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape	2021	Irlanda	La detección de anomalías grupales, el aprendizaje profundo y la teoría de grafos se combinan para identificar redes de actores malintencionados dentro de grupos generales de usuarios y clientes.
5	Alexios Mylonas, Christos Chrysoulas, Sokratis Katsikas, Nikolaos Pitropakis, Pavlos Papadopoulos y Michael Gallagher	Investigating Machine Learning attacks on financial time series models	2022	Reino Unido	El campo de Adversarial Machine Learning estudia cómo un atacante podría explotar esta característica y las contramedidas para defenderse de ellos. Este trabajo examina el ataque Fast Gradient Signed Method (FGSM).
6	Finenko Yuriy, Nikodem Joanna, Veselska Olga y Ziubina Ruslana	Big Data Analysis Methods Based on Machine Learning to Ensure Information Security	2021	Polonia	Se consideran las posibilidades de aplicación de algoritmos de aprendizaje automático con el objetivo de salvaguardar los sistemas de información. Se ofrece el concepto de construir un nuevo método de análisis de información primaria.

7	Çağlayan MAH., Bahtiyar S.	Money Laundering Detection with Node2Vec	2022	Turquía	Realizaron una representación de datos basada en gráficos con Node2Vec para tener mejores resultados de clasificación para las detecciones de lavado de dinero con algoritmos de aprendizaje automático.
8	Joel Runevic, Andreas Weber, Branka Stojanović, Atta Badii, Kai Nahrgang, Katharina Hofer-Schmitz, Josip Božić y Maheshkumar Sundaram y Elliot Jordan	Trajectory Tracing: Machine Learning for Fraud Detection in FinTech Applications	2021	Suiza	Se aplican técnicas del área de Machine Learning (ML) para identificar anomalías en aplicaciones Fintech. Apuntan a actividades sospechosas en conjuntos de datos financieros y generan modelos para anticipar futuros fraudes.
9	Adamu Sani Yahaya, Ibrahim A. Hameed, Ashfaq Tehreem, Sheraz Aslam, Safa Alsafar, Rabiya Khalid y Ahmad Taher Azar	Efficient Machine Learning and Fraud Detection Mechanisms in Blockchain	2022	Suiza	Existen dos algoritmos de aprendizaje automático, XGboost y Random Forest (RF), que se utilizan para la clasificación de transacciones. Los modelos de aprendizaje automático instruyen al conjunto de datos mediante los modelos de fraude previos y los esquemas de transacciones identificados, lo que les permite predecir las transacciones nuevas que se presentan.
10	Chenhao Li, Hui He, Ran An, Tao Liu, Liangliang Lin, Zhi Wang y Hui He	Efficient and Secure Federated Learning for Financial Applications	2023	China	Utiliza el aprendizaje federado que es una configuración de aprendizaje automático que puede proteger la privacidad de los datos, pero el alto costo de la comunicación suele ser el cuello de botella de los sistemas federados, especialmente para las grandes redes neuronales.
11	Gonzalez Diez Héctor,	Algoritmos de detección de	2021	Cuba	Se llevó a cabo un examen exhaustivo de los algoritmos fundamentales para detectar

	Ameijeiras Sanchez David y Valdes Suarez Odeynis	anomalías con redes profundas. Revisión para detección de fraudes bancarios.			irregularidades utilizando técnicas de aprendizaje profundo, específicamente enfocadas en la identificación de actividades fraudulentas en el ámbito bancario.
12	Prudhvi Parne	Artificial Intelligence and Machine Learning Role in Financial Services	2021	Estados Unidos	Los datos de las transacciones financieras son una mina de oro para muchas organizaciones. Estas usan el aprendizaje automático para crear algoritmos que cambian la forma de protección y seguridad de la información financiera.

Con respecto a los países que están dentro del estudio de investigación, se demuestra que este tema es importante para los continentes de América, Asia y Europa. La Figura 3 muestra la cantidad de investigaciones por países que participan en este estudio.

Figura 3. Número de artículos publicados por país.

La información financiera

De acuerdo con Prudhvi (2021), el sector financiero es un objetivo principal para los atacantes debido a la sensibilidad de la información disponible. Las entidades financieras tienen la capacidad de emplear tecnologías como el aprendizaje automático, para identificar potenciales amenazas mediante el análisis de firmas, patrones y anomalías detectadas. También es posible identificar de manera efectiva anomalías en las transacciones al mapear varios aspectos de la información con la información histórica, así como analizar las actividades de los usuarios para definir actividades más allá de sus roles y responsabilidades que puedan representar un riesgo. Asimismo, se pueden identificar posibles soluciones que reduzcan los riesgos de seguridad.

El aprendizaje automático en la seguridad de la información

Según Narsimha et al. (2022), destaca que los investigadores de informática buscan constantemente desarrollar nuevas técnicas y aplicaciones de sistemas, y que la inteligencia artificial (IA) es una herramienta fundamental para lograrlo. La IA se puede utilizar para diseñar máquinas inteligentes, y tiene una amplia variedad de aplicaciones en diferentes campos. La protección de datos es un ámbito en el cual se emplean estrategias de inteligencia artificial, incluyendo el uso de metodologías de aprendizaje automático y tiene como finalidad gestionar vulnerabilidades, predecir riesgos, detectar amenazas y prevenir intrusiones. Se considera que el Machine Learning tiene un gran potencial para prevenir y detectar desviaciones relacionadas con la protección de datos financieros como el fraude y otros delitos cibernéticos (Figura 4).

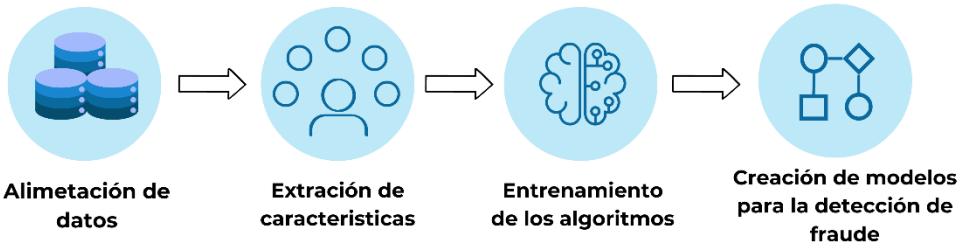

Figura 4. Proceso de Machine Learning en la creación de modelos de seguridad financiera.

Adaptado de: Narsimha et al (2023)

Métodos recurrentes para la detección del fraude financiero

Para la detección de posibles problemas de seguridad de información financiera con Machine Learning se ha recopilado en la figura los métodos más usados para la detección de fraude financiero. Estos permiten que los diferentes tipos de peligro que pueda sufrir la entidad bancaria sean detectados a tiempo con el fin de evitar mayores dificultades para la institución financiera, así como también para sus clientes.

Figura 5. Métodos de detección de fraude financiero usando Machine Learning.

Importancia de la herramienta de aprendizaje automático en la protección de los datos financieros

Para comprender la relevancia del empleo del Aprendizaje Automático en las instituciones financieras para la seguridad de la información, tenemos primero la investigación de Gallagher et al. (2022) donde se extrae que la importancia del aprendizaje automático para este problema radica en que las series temporales financieras son datos complejos y dinámicos que requieren

de modelos precisos y confiables para su análisis y predicción. El Machine Learning posibilita la identificación de pautas y corrientes de información en estos datos, brindando respaldo en la toma de decisiones tanto por parte de seres humanos como de sistemas autónomos.

Por otro lado, el lavado de dinero radica en que esta actividad criminal es una amenaza importante para las instituciones financieras y las sociedades. Según Caglayan et al. (2022) menciona que, con el uso de la tecnología, el lavado de dinero se ha vuelto más complejo y sofisticado, lo que hace que sea difícil detectarlo con los métodos tradicionales. Es por ello que el aprendizaje automático permite analizar grandes volúmenes de datos financieros y extraer patrones que ayuden a identificar las transacciones anómalas o sospechosas de lavado de dinero. Al detectar estas transacciones, las instituciones financieras pueden tomar medidas preventivas y minimizar las pérdidas económicas para los clientes y las mismas instituciones.

Así mismo, Gallagher et al. (2022) propone una solución innovadora y eficiente para el problema del fraude en las transacciones con criptomonedas, que es un fenómeno cada vez más frecuente y perjudicial para la economía y la seguridad. Al utilizar estas tecnologías juntas se puede crear un mecanismo de detección de fraudes que es preciso, robusto y resistente a ataques, aquello que impulsa el progreso del saber científico en el ámbito de la inteligencia artificial enfocada en la protección financiera.

Ahora bien, la importancia del aprendizaje federado que es una técnica del Machine Learning en las aplicaciones financieras radica en que permite entrenar modelos de aprendizaje automático de forma colaborativa y descentralizada, sin comprometer la privacidad o seguridad de los datos distribuidos en múltiples entidades. Según el estudio de Liu et al. (2023) el aprendizaje federado es una solución eficiente para abordar los desafíos de privacidad y seguridad en el proceso de capacitación de modelos de Machine Learning en sistemas financieros, mejorando la precisión y generalización de estos.

Finalmente, la importancia de la aplicación del Machine Learning en las entidades financieras es que permite usando modelos optimizados la identificación de patrones, tendencias en series temporales financieras y operaciones financieras que generen fraudes en transacciones. Además, el aprendizaje federado ofrece una solución eficiente para entrenar modelos de forma colaborativa y descentralizada sin comprometer la privacidad y seguridad de los datos distribuidos en múltiples entidades financieras. En conjunto, estos beneficios hacen que la aplicación del aprendizaje automático en instituciones financieras sea crucial para optimizar la seguridad de la información y advertir actividades ilegales que puedan afectar a la economía y a la sociedad en general.

Conclusiones

Tras un minucioso análisis acerca de la relevancia del Aprendizaje Automático en la protección de la información financiera, se puede concluir que esta tecnología es relevante porque es uno de los recursos más empleados para combatir el fraude financiero y otras potenciales vulnerabilidades que representan una amenaza para la protección de la información económica de las empresas.

En este contexto, se infiere que existen muchos ciberdelincuentes que aprovechan las debilidades de los sistemas financieros para extraer información confidencial o realizar transacciones fraudulentas que les permiten obtener ganancias ilegales. Ante esta situación el sector financiero necesita contar con herramientas efectivas para combatir estos peligros y prevenirlos.

La revisión sistemática llevada a cabo en esta investigación ha permitido identificar los métodos del Machine Learning que se utilizan para la detección del fraude financiero y diferentes circunstancias que generan peligro para la confidencialidad de los datos en el ámbito financiero. Estas tecnologías son efectivas para detectar patrones y anomalías en los datos financieros, lo que permite a las instituciones financieras tomar medidas preventivas antes de que ocurran situaciones críticas.

Es importante mencionar que, para el futuro, estas tecnologías del Machine Learning seguirán evolucionando, llegando a su máximo potencial. En este sentido, los sistemas financieros deben implementar estas herramientas tecnológicas para optimizar su seguridad de la información y evitar posibles riesgos de fraudes financieros. Así, se logrará garantizar la tranquilidad de los colaboradores y clientes de las instituciones financieras.

Referencias Bibliográficas

Arnau, L., y Sala, J. (2020). La revisión de la literatura científica: Pautas, procedimientos y criterios de calidad. Recuperado el 20 de junio 2021, del sitio web de la Universidad Autónoma de Barcelona: https://ddd.uab.cat/pub/recdoc/2020/222109/revliltcie_a2020.pdf

Bahtiyar, Ş., & Çağlayan, M. (2022). Money laundering detection with Node2Vec. Gazi University Journal of Science, 35(3), 854-873. https://doi.org/10.35378/gujs.854725

Boden, M. (2017). Inteligencia artificial. Turner.

Bobyk, A., Srokosz, M., Ksiezopolski, B., & Wydra, M. (2023). Machine-Learning-Based Scoring System for Antifraud CISIRTs in Banking Environment. Electronics, 12(1), 251. https://doi.org/10.3390/electronics12010251

Bonfill, X., & Urrútia, G. (2010). Declaración PRISMA: Una propuesta para mejorar la publicación de revisiones sistemáticas y metaanálisis. Medicina Clínica, 135(11), 507-511. https://doi.org/10.1016/j.medcli.2010.01.015

Božić, J., Stojanović, B., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., Sundaram, M., et al. (2021). Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications. Sensors, 21(5), 1594. http://dx.doi.org/10.3390/s21051594

Calderón, L. (2015). Seguridad informatica y Seguridad de la información. Universidad Piloto de Colombia. Recuperado de http://repository.unipiloto.edu.co/handle/20.500.12277/2821

Chrysoulas, C., Gallagher, M., Katsikas, S., Pitropakis, N., Papadopoulos, P., & Mylonas, A. (2022). Investigating Machine Learning attacks on financial time series models. Computers & Security, 123, 102933. https://doi.org/10.1016/j.cose.2022.102933

Domancic, S., Cuellar, J., Moreno, B., Muñoz, M., & Villanueva, J. (2018). Systematic Reviews: definition and basic notions. Revista clínica de periodoncia, implantología y rehabilitación oral, 11(3), 184-186. https://dx.doi.org/10.4067/S0719-01072018000300184

Finenko, Y., Nikodem, J., Veselska, O., Ziubina, R., & (2021). Big Data Analysis Methods Based on Machine Learning to Ensure Information Security. Procedia Computer Science, 192, 2633-2640. https://doi.org/10.1016/j.procs.2021.09.033

Hinestroza Ramírez, D. (2018). El Machine Learning a través de los tiempos, y los aportes a la humanidad. Recuperado de: https://hdl.handle.net/10901/17289

Khalid, R., Aslam, S., Ashfaq, T., Yahaya, A. S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A Machine Learning and Blockchain Based Efficient Fraud Detection Mechanism. Sensors, 22(19), 7162. https://doi.org/10.3390/s22197162

Le-Khac, N. -A., Kuppa, A., & Nicholls, J. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. IEEE Access, 9, 163965-163986. https://doi.org/10.1109/ACCESS.2021.3134076

Li, C., Shi, W., Liu, T., Wang, Z., He, H., Lin, L., & An, R. (2023). Efficient and secure federated learning for financial applications. Applied Sciences, 13(10), 5877. https://doi.org/10.3390/app13105877

Prudhvi, P. (2021). Artificial Intelligence & Machine Learning Role in Financial Services. Recuperado de https://aircconline.com/csit/papers/vol11/csit111504.pdf

Rajyalakshmi, P., Raghavendran, C. V., Narsimha, B., Reddy, G. K., Bhargavi, M., & Naresh, P. (2022). Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application. IJEER, 10(2), 87-92. https://doi.org/10.37391/IJEER.100206

Shah, V. (2022). How efficient is Machine Learning in detecting financial fraud using mobile transaction metadata? Journal of Student Research, 11(3), 2865. https://doi.org/10.47611/jsrhs.v11i3.2865

Valdés Suárez, O., Ameijeiras Sánchez, D., & González Diez, H. (2021). Algoritmos de detección de anomalías con redes profundas. Revisión para detección de fraudes bancarios. Revista Cubana de Ciencias Informáticas, 15(4, Supl. 1), 244-264. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992021000500244