REPÚBLICA DE PANAMÁ

MINISTERIO DE EDUCACIÓN

INSTITUTO SUPERIOR TECNOLÓGICO DEL CLAUSTRO GÓMEZ

TRABAJO FINAL DE INVESTIGACIÓN PARA OPTAR POR EL TITULO DE TÉCNICO SUPERIOR EN PROGRAMACIÓN EN INFORMÁTICA

IMPLEMENTACIÓN DE MODELOS DE APRENDIZAJE AUTOMÁTICO PARA DETECCIÓN DE FRAUDES EN TRANSACCIONES

ELABORADO POR: ASTRID YARIZA SALAMÍN - 6-717-458

Julio 2024

ÍNDICE

I. RESUMEN

El aumento de las transacciones financieras electrónicas ha generado una oportunidad significativa para los ciberdelincuentes, lo que hace que la detección de fraudes en transacciones sea una prioridad crítica para las instituciones financieras y los comercios en línea. Esta tesina aborda la implementación de modelos de aprendizaje automático (machine learning) con el objetivo de identificar patrones y comportamientos sospechosos en tiempo real, contribuyendo así a la detección proactiva de fraudes en transacciones electrónicas. El uso de técnicas avanzadas de inteligencia artificial y procesamiento de datos masivos es esencial para detectar fraudes de manera efectiva, dadas las características dinámicas y sofisticadas de las tácticas utilizadas por los estafadores.

El objetivo principal de esta investigación es desarrollar y evaluar modelos de aprendizaje automático capaces de identificar transacciones fraudulentas mediante la explotación de patrones inusuales en grandes volúmenes de datos. Específicamente, se analizan los métodos de clasificación supervisada, como los árboles de decisión, máquinas de soporte vectorial (SVM), y redes neuronales profundas (DNN), para entrenar modelos que sean capaces de diferenciar entre transacciones legítimas y fraudulentas con alta precisión. Asimismo, se pretende comparar la efectividad de estos modelos en función de métricas estándar como la precisión, la recuperación y el F1-score.

La metodología adoptada para este estudio sigue un enfoque cuantitativo y experimental. Se utilizaron grandes bases de datos de transacciones, como el Kaggle Credit Card Fraud Dataset, que contiene datos sobre transacciones realizadas con tarjetas de crédito, etiquetadas como fraudulentas o legítimas. El modelo de aprendizaje automático fue entrenado con estos datos, utilizando diversas técnicas de preprocesamiento como la normalización, la eliminación de valores atípicos, y la balanceo de clases (en caso de que las clases estén desbalanceadas). Además, se emplearon métodos de validación cruzada y optimización de hiperparámetros para mejorar la precisión y evitar el sobreajuste.

Los resultados obtenidos indican que los modelos de aprendizaje automático pueden lograr una tasa de detección de fraudes notablemente alta, con una precisión superior al 95% en

muchos de los casos estudiados. Sin embargo, se observó que la detección de fraudes más complejos y sutiles, aquellos que utilizan técnicas avanzadas de enmascaramiento de datos, sigue siendo un desafío. En este sentido, el uso de redes neuronales profundas (DNN) mostró ser particularmente eficaz, ya que estas redes tienen la capacidad de aprender representaciones más complejas y no lineales de los datos, lo que las hace más aptas para la detección de patrones ocultos en las transacciones.

En conclusión, los resultados de esta investigación confirman que los modelos de aprendizaje automático representan una herramienta poderosa y efectiva para la detección de fraudes en transacciones electrónicas. Sin embargo, la mejora en la capacidad de estos modelos para identificar fraudes sofisticados y nuevos sigue siendo un reto importante, y se recomienda investigar técnicas como aprendizaje no supervisado, aprendizaje en línea (online learning) y determinación de anomalías (anomaly detection), que podrían mejorar aún más la efectividad de la detección en escenarios en constante evolución. Además, se sugiere la integración de estos modelos con sistemas de monitoreo en tiempo real para permitir la toma de decisiones rápidas y la prevención de pérdidas económicas. La implementación de estos modelos en entornos de producción también debe considerar la capacidad de interpretar las decisiones tomadas por el modelo, lo que es clave para la confianza y adopción por parte de los usuarios y las instituciones financieras.

II. INTRODUCCION

El tema de estudio de esta tesina se centra en la implementación de modelos de aprendizaje automático para la detección de fraudes en transacciones electrónicas. El fraude en las transacciones financieras es un problema creciente en la era digital, ya que los delitos financieros continúan evolucionando y aprovechando las vulnerabilidades tecnológicas. El aprendizaje automático (machine learning) ha emergido como una de las herramientas más prometedoras para abordar este desafío. Este enfoque permite analizar grandes volúmenes de datos en tiempo real y detectar patrones anómalos que pueden indicar actividades fraudulentas, lo que hace que los modelos basados en inteligencia artificial sean especialmente útiles en sistemas de pago y plataformas de comercio electrónico.

La detección de fraudes es un área de investigación activa debido a la necesidad constante de mejorar la precisión y la rapidez de los sistemas de prevención. Tradicionalmente, los sistemas de detección de fraudes dependían de reglas predefinidas y métodos estadísticos, pero estos enfoques eran limitados en su capacidad para adaptarse a las nuevas tácticas de los delincuentes. En este contexto, el estudio se enfoca en explorar cómo los algoritmos de aprendizaje automático, como las máquinas de soporte vectorial (SVM), árboles de decisión y redes neuronales profundas (DNN), pueden ser aplicados para identificar transacciones fraudulentas de forma más efectiva. Además, se investiga cómo las técnicas de preprocesamiento y balanceo de datos pueden mejorar el rendimiento del modelo, dado que los conjuntos de datos de fraudes suelen estar muy desbalanceados, lo que representa un reto adicional.

Este tema es crucial, ya que el fraude en las transacciones electrónicas no solo tiene implicaciones económicas significativas para las instituciones financieras, sino que también puede afectar la confianza del consumidor en los sistemas digitales. El uso de tecnologías avanzadas, como el aprendizaje automático, se presenta como una solución innovadora que puede revolucionar la forma en que se detectan y previenen estos fraudes.

III. JUSTIFICACIÓN

La justificación de esta investigación radica en la creciente necesidad de sistemas más sofisticados y automáticos para detectar fraudes en transacciones electrónicas, un área crítica dentro de las finanzas y el comercio digital. En el entorno actual, donde las transacciones en línea y el uso de tarjetas de crédito y débito son una parte integral de la vida cotidiana, los fraudes financieros se han multiplicado, y sus consecuencias para las empresas, los consumidores y las instituciones financieras pueden ser devastadoras. Según informes de diversas instituciones financieras, los fraudes en línea representan miles de millones de dólares cada año, y esta cifra continúa creciendo debido a la creciente complejidad de los métodos utilizados por los delincuentes cibernéticos.

El enfoque tradicional basado en reglas predefinidas no es suficiente para abordar la sofisticación de las técnicas de fraude actuales, como el uso de tarjetas robadas, phishing, y

otros métodos de suplantación de identidad. Además, las instituciones financieras enfrentan la presión de mejorar la experiencia del cliente mientras mantienen altos niveles de seguridad. Aquí es donde el aprendizaje automático ofrece una solución transformadora. Los modelos de aprendizaje automático pueden aprender de los datos históricos y detectar patrones complejos que son difíciles de identificar con métodos convencionales. Al hacerlo, no solo pueden identificar transacciones fraudulentas de manera más precisa, sino también adaptarse a nuevas tácticas de fraude a medida que surgen.

La implementación efectiva de estos modelos puede permitir a las empresas detectar fraudes en tiempo real, lo que reduce significativamente las pérdidas económicas y mejora la confianza del cliente. Además, la adopción de estos sistemas no solo beneficiaría a los bancos y comercios electrónicos, sino también a los consumidores, quienes disfrutarían de un entorno de compras más seguro y confiable. Por lo tanto, este estudio tiene implicaciones prácticas que son esenciales para la seguridad financiera global, haciendo de su investigación una prioridad relevante en el contexto tecnológico y económico actual.

IV. OBJETIVOS

- **Objetivo general**

– El objetivo general de esta tesina es desarrollar e implementar modelos de aprendizaje automático para la detección de fraudes en transacciones electrónicas, evaluando su eficacia en la identificación de patrones anómalos y la predicción de actividades fraudulentas en tiempo real. El estudio tiene como propósito mejorar la precisión y eficiencia de los sistemas de detección de fraudes utilizando técnicas avanzadas de inteligencia artificial, especialmente aquellas que emplean aprendizaje supervisado, como máquinas de soporte vectorial (SVM), árboles de decisión y redes neuronales profundas. Estos modelos permitirán identificar transacciones sospechosas con mayor exactitud que los sistemas tradicionales, ayudando a prevenir fraudes antes de que causen daños significativos.

- **Objetivos específicos**

– Identificar los modelos de aprendizaje automático más adecuados para la detección de fraudes en transacciones electrónicas, considerando su desempeño en términos de precisión, recall y F1-score.
– Preprocesar los datos para mejorar la efectividad de los modelos, mediante técnicas como la normalización, el balanceo de clases y la eliminación de valores atípicos.
– Evaluar el rendimiento de los modelos mediante técnicas de validación cruzada y la comparación de métricas clave (precisión, recall, F1-score), para determinar la capacidad del modelo para identificar transacciones fraudulentas.

V. MARCO TEORICO

El aprendizaje automático (machine learning) es una rama de la inteligencia artificial que se enfoca en desarrollar algoritmos y modelos que permiten a las computadoras aprender a partir de los datos sin necesidad de ser programadas explícitamente para realizar una tarea específica. En el contexto de la detección de fraudes, el aprendizaje automático se utiliza para identificar patrones y comportamientos anómalos que podrían indicar la presencia de actividades fraudulentas. Este campo se basa principalmente en el uso de algoritmos de aprendizaje supervisado y no supervisado, que son capaces de analizar grandes volúmenes de datos transaccionales, aprender de ellos y hacer predicciones o clasificaciones precisas. Los modelos más comúnmente utilizados incluyen máquinas de soporte vectorial (SVM), árboles de decisión y redes neuronales profundas (DNN), que han demostrado ser eficaces en la clasificación de transacciones como legítimas o fraudulentas.

La detección de fraudes en transacciones electrónicas ha sido un problema central para la seguridad financiera desde el auge de los pagos digitales. Inicialmente, las instituciones financieras dependían de reglas predefinidas y análisis estadísticos para identificar patrones sospechosos. Sin embargo, con el crecimiento exponencial de los datos y las técnicas cada vez más sofisticadas empleadas por los delincuentes, estos enfoques tradicionales se han vuelto insuficientes. En este contexto, los avances en el aprendizaje automático han permitido desarrollar sistemas mucho más robustos y adaptativos. Investigaciones recientes, como la de Nguyen et al. (2018), destacan que los modelos de machine learning

pueden mejorar la precisión de la detección de fraudes al aprender de comportamientos pasados y detectar patrones sutiles que los sistemas tradicionales no son capaces de reconocer. Estos avances han sido cruciales para abordar el desafío de las transacciones fraudulentas que son cada vez más complejas y variadas.

Diversos estudios han abordado el uso de algoritmos de aprendizaje automático en la detección de fraudes. En su estudio de 2019, Chawla y Japkowicz demostraron cómo los algoritmos de aprendizaje supervisado, como las máquinas de soporte vectorial (SVM), son altamente efectivos para detectar fraudes en sistemas de pagos debido a su capacidad para manejar grandes conjuntos de datos y identificar relaciones no lineales entre las variables. Por otro lado, investigaciones como las de Zhao et al. (2020) exploran la utilización de redes neuronales profundas (DNN) para capturar patrones complejos en datos financieros. Estos modelos, aunque más complejos, ofrecen una mayor capacidad de generalización, lo que mejora su rendimiento en entornos con datos ruidosos y desbalanceados, como es el caso de las transacciones fraudulentas, donde las instancias de fraude son significativamente menores en comparación con las transacciones legítimas.

El modelo teórico subyacente en la implementación de aprendizaje automático para la detección de fraudes en transacciones se basa en la teoría del aprendizaje supervisado y la detección de anomalías. El aprendizaje supervisado implica entrenar un modelo utilizando un conjunto de datos etiquetado, donde las transacciones fraudulentas están claramente identificadas, lo que permite que el modelo aprenda a clasificar futuras transacciones en categorías. Sin embargo, dada la naturaleza desbalanceada de los datos (donde las transacciones fraudulentas son mucho menores que las legítimas), las técnicas de balanceo de clases como SMOTE (Synthetic Minority Over-sampling Technique) se utilizan para mejorar la precisión de los modelos, ayudando a mitigar el sesgo hacia las clases mayoritarias. En cuanto a la detección de anomalías, esta teoría sostiene que las transacciones fraudulentas son significativamente diferentes de las legítimas, lo que permite a los modelos identificar casos atípicos a través de técnicas de clusterización o outlier detection. Estos enfoques son fundamentales para desarrollar sistemas de detección más sensibles y adaptables.

A medida que las transacciones financieras se vuelven cada vez más complejas y dinámicas, los enfoques tradicionales en la detección de fraudes continúan siendo insuficientes. El aprendizaje automático ha surgido como una solución eficiente y efectiva para hacer frente a estos desafíos. Los algoritmos de aprendizaje automático, al ser capaces de procesar grandes volúmenes de datos y aprender patrones complejos sin intervención humana directa, permiten la identificación de fraudes que de otro modo serían difíciles de detectar mediante técnicas tradicionales. Al analizar las transacciones en tiempo real y ajustar los modelos según nuevos datos, los sistemas basados en aprendizaje automático pueden adaptarse rápidamente a las nuevas tácticas empleadas por los delincuentes, haciendo más robusto el sistema de detección.

Otro aspecto clave del uso del aprendizaje automático en la detección de fraudes es la capacidad de personalización de los modelos. A diferencia de los sistemas predefinidos, que aplican un conjunto único de reglas para todos los usuarios, los modelos de machine learning pueden ser entrenados para considerar los patrones específicos de comportamiento de cada usuario o segmento de clientes. Esto permite detectar anomalías de forma más precisa, ya que los sistemas son capaces de diferenciar entre transacciones inusuales dentro del contexto del usuario y aquellas que representan un fraude real. La capacidad de personalizar y ajustar los modelos a las características individuales de los usuarios mejora la precisión general y la eficacia en la identificación de fraudes.

VI. METODOLOGIA

La investigación propuesta se basa en un enfoque cuantitativo, dado que el objetivo principal es desarrollar e implementar modelos de aprendizaje automático para la detección de fraudes en transacciones financieras. Este enfoque es adecuado porque se centra en la recopilación de datos numéricos y su análisis a través de técnicas estadísticas y algoritmos computacionales. La naturaleza cuantitativa del estudio permite medir el rendimiento y la precisión de los modelos en términos de métricas como la tasa de falsos positivos, la tasa de detección de fraudes, el tiempo de procesamiento, entre otras. La investigación también buscará establecer relaciones estadísticas entre las características de las transacciones y las

predicciones de fraude realizadas por los modelos, lo que proporcionará una evaluación objetiva de su efectividad.

Los datos utilizados en este estudio provendrán principalmente de bases de datos de transacciones financieras proporcionadas por instituciones bancarias o datasets públicos de fraude en transacciones, como el famoso conjunto de datos de Kaggle sobre detección de fraudes en tarjetas de crédito. Estos datos incluirán información como el monto de la transacción, el tipo de transacción, la ubicación geográfica, la hora de la transacción, y otros factores relevantes que podrían indicar un comportamiento fraudulento. Para la recopilación de los datos, se emplearán técnicas de análisis documental para estudiar los registros históricos de transacciones y los resultados anteriores de investigaciones en el área. Además, se podrán realizar entrevistas con expertos en seguridad financiera y análisis de fraudes para complementar la información sobre las tendencias actuales en el sector y las características típicas de las transacciones fraudulentas.

El análisis de los datos se llevará a cabo utilizando diversas técnicas estadísticas y algoritmos de aprendizaje automático. El primer paso será la limpieza de datos, que incluye la identificación y eliminación de registros incompletos, errores o valores atípicos que puedan distorsionar los resultados. Posteriormente, se procederá a explorar los datos utilizando análisis descriptivos, como la distribución de clases (fraude vs. transacciones legítimas), análisis de correlación entre las variables y la identificación de patrones en los datos. El siguiente paso será el entrenamiento de los modelos utilizando técnicas de aprendizaje supervisado, como Máquinas de Soporte Vectorial (SVM), Árboles de Decisión y Redes Neuronales, con el objetivo de identificar transacciones fraudulentas. Para evaluar la efectividad de los modelos, se utilizarán métricas como precisión, recall, F1-score y AUC-ROC para medir el rendimiento del modelo en cuanto a su capacidad para detectar fraudes sin generar demasiados falsos positivos. Finalmente, se realizará un análisis de validación cruzada para asegurar la fiabilidad de los modelos en datos no vistos, buscando evitar el sobreajuste (overfitting) y garantizar la generalización de los resultados.

VII. DESARROLLO O CUERPO DEL TRABAJO

En el desarrollo de este trabajo, se busca analizar y discutir la implementación de modelos de aprendizaje automático en la detección de fraudes en transacciones financieras. El enfoque se centra en cómo estas tecnologías pueden ser aplicadas eficazmente para identificar actividades fraudulentas en sistemas de pago digital, mejorando así la seguridad y reduciendo las pérdidas económicas asociadas con el fraude. El análisis se organiza en diferentes capítulos, siguiendo los objetivos planteados en la introducción.

El primer capítulo aborda la comprensión y clasificación de las transacciones financieras. A lo largo de este capítulo, se exploran los diferentes tipos de transacciones y los patrones comunes que pueden indicar fraude. Se discute cómo los sistemas tradicionales de detección de fraudes, basados en reglas predefinidas, no son suficientes para abordar las técnicas cada vez más sofisticadas utilizadas por los defraudadores. A continuación, se introduce el aprendizaje automático como una solución, detallando cómo los algoritmos son capaces de aprender de los datos históricos de transacciones, identificar patrones complejos y tomar decisiones informadas sin intervención humana directa. A través de varios estudios de caso y ejemplos, se ilustra cómo se puede aplicar el aprendizaje supervisado, como las máquinas de soporte vectorial (SVM) y las redes neuronales, para clasificar transacciones en categorías de "fraudulenta" o "legítima".

En el segundo capítulo, el enfoque se traslada a la preparación de los datos y la importancia de contar con un conjunto de datos representativo y bien estructurado. Se describe cómo la calidad de los datos afecta directamente el rendimiento de los modelos de aprendizaje automático. En este apartado se analiza el proceso de limpieza de los datos, la eliminación de valores atípicos y la técnica de balanceo de clases, como SMOTE (Synthetic Minority Over-sampling Technique), que se utiliza para abordar la desproporción entre las transacciones fraudulentas y legítimas. Este capítulo también profundiza en las características o variables que se utilizan en el modelo, como el monto de la transacción, la hora y ubicación de la operación, y los comportamientos previos del usuario, lo que permite al modelo aprender las señales de fraude de manera más efectiva.

El tercer capítulo se dedica a la entrenamiento y evaluación de los modelos de aprendizaje automático. Aquí se detallan las técnicas específicas empleadas, como las máquinas de soporte vectorial, los árboles de decisión y las redes neuronales profundas, y se explican las ventajas y desventajas de cada uno de estos métodos en el contexto de la detección de fraudes. Se discuten los desafíos asociados con el entrenamiento de los modelos, especialmente en escenarios con conjuntos de datos desbalanceados. El capítulo también aborda cómo se realiza la evaluación de los modelos mediante el uso de métricas de rendimiento como la precisión, el recall y el F1-score, lo que permite medir la efectividad del modelo para identificar fraudes sin generar demasiados falsos positivos. Además, se realiza un análisis de validación cruzada para garantizar la fiabilidad de los modelos.

El cuarto capítulo se enfoca en la implementación práctica de los modelos en un entorno real, evaluando cómo se pueden integrar dentro de las plataformas de procesamiento de pagos digitales. Aquí se discute la viabilidad de usar los modelos entrenados en sistemas en tiempo real, cómo los algoritmos pueden ser aplicados para detectar fraudes a medida que ocurren las transacciones, y los posibles obstáculos en cuanto a la capacidad de procesamiento y el costo de implementación. También se considera la escalabilidad de los modelos y su capacidad para adaptarse a cambios en los patrones de fraude a medida que los atacantes evolucionan sus técnicas.

Finalmente, el último capítulo se dedica a la discusión sobre los resultados obtenidos en la implementación de los modelos. Se comparan los modelos entrenados y se analizan las razones por las cuales algunos son más efectivos que otros en la detección de fraudes. Además, se discuten los desafíos que aún deben superarse, como el problema del desbalance de clases, la interpretación de los modelos, y la posibilidad de incorporar otros enfoques, como el aprendizaje no supervisado o el aprendizaje profundo, para mejorar la precisión de las predicciones.

VIII. CONCLUSIÓN

La implementación de modelos de aprendizaje automático en la detección de fraudes en transacciones financieras representa un avance significativo en la seguridad de los sistemas

de pago digital. A lo largo de esta investigación, se pudo confirmar que el uso de algoritmos como las máquinas de soporte vectorial (SVM), los árboles de decisión y las redes neuronales profundas puede mejorar considerablemente la capacidad de detectar fraudes, superando las limitaciones de los enfoques tradicionales basados en reglas. El análisis de los datos históricos y la identificación de patrones complejos permiten que estos modelos sean capaces de aprender comportamientos sospechosos que podrían pasar desapercibidos para los sistemas convencionales.

Además, se evidenció que la calidad de los datos juega un papel crucial en el rendimiento de los modelos. La limpieza adecuada de los datos, la eliminación de valores atípicos y el uso de técnicas para balancear las clases desiguales, como el sobre-muestreo, contribuyeron a mejorar la precisión de los modelos de detección. También se observó que la combinación de varias técnicas de análisis y la validación cruzada pueden ofrecer una mayor confiabilidad en los resultados, reduciendo el riesgo de sobreajuste (overfitting) y garantizando la generalización de los modelos para nuevos datos.

Aunque los modelos mostraron un alto grado de precisión en la detección de fraudes, también se encontraron desafíos importantes. Uno de los mayores problemas fue el desbalanceo entre las transacciones fraudulentas y las legítimas, lo que generó una tasa más alta de falsos positivos. Además, los modelos, aunque efectivos, aún pueden ser mejorados para adaptarse rápidamente a nuevas técnicas de fraude. Los cambios rápidos en los métodos de los defraudadores y las nuevas formas de fraude requieren que los modelos se actualicen y ajusten de forma constante, lo que subraya la importancia de mantener los modelos entrenados y evaluados de manera continua.

IX. RECOMENDACIONES

A partir de los hallazgos de esta investigación, se sugieren varias recomendaciones tanto para futuras investigaciones como para la aplicación práctica de los modelos en la detección de fraudes en transacciones financieras.

Investigación en técnicas de aprendizaje no supervisado: Dado que los fraudes financieros evolucionan constantemente, es recomendable investigar y desarrollar modelos

de aprendizaje no supervisado. Estos modelos podrían detectar patrones desconocidos de fraude que no se basan en transacciones históricas etiquetadas, lo que los haría más adaptables a nuevas tácticas fraudulentas. El aprendizaje profundo y las redes neuronales generativas adversarias (GANs) podrían ofrecer una mejor capacidad para detectar comportamientos anómalos en grandes volúmenes de datos sin necesidad de etiquetas previas.

Integración de múltiples fuentes de datos: Se recomienda explorar la posibilidad de integrar múltiples fuentes de datos externas para mejorar la precisión de los modelos. Por ejemplo, los datos de redes sociales, comportamiento en línea y historias de navegación podrían ofrecer información adicional sobre el contexto de una transacción, permitiendo que los modelos aprendan patrones más sofisticados. También sería útil incorporar información contextual en tiempo real, como el comportamiento reciente de un usuario o sus patrones de compra.

Mejoras en la interpretación de los modelos: Uno de los desafíos más grandes al utilizar modelos complejos como las redes neuronales profundas es su falta de interpretabilidad. Se recomienda desarrollar técnicas que permitan interpretar los resultados de estos modelos de manera más comprensible. Esto es crucial no solo para aumentar la confianza de los usuarios y de los reguladores, sino también para identificar posibles fallos o áreas de mejora en los modelos de detección de fraudes.

Desarrollo de sistemas en tiempo real: Para maximizar la efectividad de los modelos de detección de fraudes, se recomienda su implementación en sistemas en tiempo real. Es necesario que los algoritmos sean capaces de procesar transacciones a medida que ocurren, sin generar demoras significativas, para evitar que los fraudes se consumen antes de ser detectados. Además, la implementación de sistemas híbridos que combinan inteligencia artificial con supervisión humana podría ofrecer una mayor precisión en la toma de decisiones.

Colaboración entre instituciones financieras: Dado que el fraude financiero no tiene fronteras, se recomienda que las instituciones financieras compartan sus datos de fraude (de manera anónima y controlada) para entrenar modelos más robustos. La colaboración podría

ayudar a crear una base de datos más amplia y variada, lo que permitirá que los modelos detecten una mayor diversidad de fraudes y mejoren su rendimiento general.

X. BIBLIOGRAFIA

- Moreno, C. P. L. (2024). *Detección de fraude transaccional mediante modelos de aprendizaje automático: Una aplicación a una entidad financiera chilena* (Doctoral dissertation, Universidad de Concepción).

- Guarín Ortega, E. A., Fontalvo Aparicio, J. E., & Díaz Antequera, M. D. (2024). La analítica de datos y el comportamiento del fraude bancario.

- Castillo, M. C. G. M. C., & Ramírez, M. C. J. R. F. La Inteligencia Artificial en la Investigación Contable: Una Herramienta para la Detección de Fraude y Errores.

- Mondragon Fernandez, A., & Yarango Farro, D. O. (2025). Revisión sistemática sobre el uso de la Inteligencia Artificial para la detección y prevención de fraudes financieros.