UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

TESIS

"IMPLEMENTACIÓN DE UN MODELO PREDICTIVO DE APRENDIZAJE AUTOMÁTICO PARA LA DETECCIÓN TEMPRANA DE TRANSACCIONES DE LAVADO DE ACTIVOS EN ENTIDADES FINANCIERAS"

PARA OBTENER EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS

ELABORADO POR:

DONNALYN FRANCESCA MELGAR GRIJALBA

0009-0001-4341-1905

ASESOR:

DR. EMILIO ALBERTO UN JAN LIAU HING

0000-0002-7803-6236

LIMA – PERÚ

2025

Citar/How to cite	Melgar Grijalba [1]
Referencia/Reference Estilo/Style: IEEE (2020)	[1] D. Melgar Grijalba, "*Implementación de un modelo predictivo de aprendizaje automático para la detección temprana de transacciones de lavado de activos en entidades financieras*" [Tesis de pregrado]. Lima (Perú): Universidad Nacional de Ingeniería, 2025.

Citar/How to cite	(Melgar, 2025)
Referencia/Reference Estilo/Style: APA (7ma ed.)	Melgar, D. (2025). *Implementación de un modelo predictivo de aprendizaje automático para la detección temprana de transacciones de lavado de activos en entidades financieras*. [Tesis de pregrado, Universidad Nacional de Ingeniería]. Repositorio institucional Cybertesis UNI.

DEDICATORIA

El presente trabajo va dedicado con profundo amor y gratitud a:

Mi padre, Ramiro Melgar Balbin, por su gran esfuerzo incansable, su guía constante y su apoyo incondicional a lo largo de mi vida. Gracias por luchar cada día para brindarnos lo mejor y por ser siempre mi ejemplo de perseverancia.

Mi madre, Patricia Lourdes Grijalba Cañari, cuya memoria vive en mí cada día. Gracias por tu amor infinito, por ser el ejemplo de una mujer guerrera, por enseñarme a creer en mí misma, por tu compañía silenciosa en tantas noches de estudio y por seguir siendo mi inspiración desde el cielo. Tu legado siempre estará vivo en mí y en la familia. Un beso al cielo.

Mi hermana, Cristina Melgar Grijalba, por darme la valentía que necesitaba para culminar esta tesis. Gracias por tu preocupación constante y por la compañía que siempre hemos compartido.

Mi hermano, Martin Melgar Grijalba, por ser mi cómplice en los momentos de alegría, por estar siempre presente con tu energía y apoyo incondicional, ¡y también por prestarme tu laptop cuando más la necesitaba!

Y a mi familia en general, por su cariño inagotable y aliento constante en cada etapa de este camino.

Este logro no es solo mío, sino de todos ustedes. Gracias por siempre confiar en mí. ¡Los amo!

AGRADECIMIENTO

En primer lugar, deseo expresar mi más sincero agradecimiento a los docentes de la Facultad de Ingeniería Industrial y de Sistemas de la Universidad Nacional de Ingeniería, por la valiosa labor que desempeñan en la formación académica y profesional de sus estudiantes. Extiendo mi agradecimiento especial al Dr. Emilio Un Jan, Dr. Hilario Aradiel y Dr. Paul Tocto, cuya orientación y aportes han contribuido significativamente a mi desarrollo como investigadora. Asimismo, agradezco profundamente a mis compañeros del equipo de trabajo de Data y Analytics de Cumplimiento. Sus experiencias y conocimientos han enriquecido tanto mi formación teórica como práctica, y han sido fundamentales en este proceso. Finalmente, a mi familia por su apoyo incondicional, su confianza en mí y por acompañarme en la consecución de un logro más en mi vida profesional.

RESUMEN

El lavado de activos constituye una amenaza crítica para la integridad del sistema financiero, especialmente en el contexto de las instituciones bancarias, donde las cuentas corrientes y de ahorro son utilizadas como vehículos para actividades ilícitas. Esta investigación propone el desarrollo de un modelo predictivo basado en técnicas de aprendizaje automático para la detección temprana de transacciones sospechosas, con el objetivo de fortalecer los mecanismos de prevención y control en entidades financieras. Para ello, se empleó el simulador AMLSim de IBM, que genera datos sintéticos representativos de transacciones bancarias, permitiendo entrenar y evaluar distintos algoritmos de clasificación.

La metodología aplicada se fundamentó en el enfoque de MLOps para asegurar la trazabilidad y reproducibilidad del proceso. Se utilizó una muestra de 10,568 registros seleccionados de una población de más de 6 millones de transacciones mediante la técnica del muestreo aleatorio sistemático. Se implementaron y compararon siete modelos de aprendizaje automático: Regresión Logística, SVM, KNN, ANN, Árbol de Decisión, Random Forest y XGBoost. Este último obtuvo el mejor desempeño, alcanzando un AUC de 88%, precisión de 83% y recall de 73%.

Mediante un análisis comparativo pre-test y post-test se comprobó, con soporte estadístico que la implementación del modelo XGBoost mejora significativamente la detección de transacciones sospechosas en comparación con un sistema tradicional basado en reglas. Esta mejora se traduce en una reducción de falsos negativos y falsos positivos, lo que permite optimizar la labor del área de cumplimiento y reducir riesgos legales y reputacionales para la entidad financiera.

Finalmente, este trabajo demuestra que el uso de modelos avanzados de aprendizaje automático puede fortalecer significativamente los sistemas de prevención de lavado de activos, contribuyendo así al cumplimiento normativo y a la seguridad del sistema financiero.

Palabras clave: Lavado de activos, aprendizaje automático, detección de transacciones sospechosas, XGBoost, inteligencia artificial, instituciones financieras, AMLSim, precisión, recall, entidades financieras.

ABSTRACT

Money laundering constitutes a critical threat to the integrity of the financial system, especially in the context of banking institutions, where checking and savings accounts are used as vehicles for illicit activities. This research proposes the development of a predictive model based on machine learning techniques for the early detection of suspicious transactions, with the aim of strengthening prevention and control mechanisms in financial institutions. To this end, IBM's AMLSim simulator was used, which generates synthetic data representative of banking transactions, allowing the training and evaluation of different classification algorithms.

The methodology applied was based on the MLOps approach to ensure the traceability and reproducibility of the process. A sample of 10,568 records was selected from a population of more than 6 million transactions using the systematic random sampling technique. Seven machine learning models were implemented and compared: Logistic Regression, SVM, KNN, ANN, Decision Tree, Random Forest, and XGBoost. The latter performed best, achieving an AUC of 88%, precision of 83%, and recall of 73%.

Through a pre-test and post-test comparative analysis, it was statistically proven that the implementation of the XGBoost model significantly improves the detection of suspicious transactions compared to a traditional rule-based system. This improvement translates into fewer false negatives and false positives, which optimizes the work of the compliance department and reduces legal and reputational risks for the financial institution.

Finally, this work demonstrates that the use of advanced machine learning models can significantly strengthen anti-money laundering systems, thus contributing to regulatory compliance and the security of the financial system.

Keywords: Money laundering, machine learning, suspicious transaction detection, XGBoost, artificial intelligence, financial institutions, AMLSim, accuracy, recall, financial institutions.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

INTRODUCCIÓN

El lavado de activos es una problemática de alcance global que afecta gravemente la integridad, estabilidad y transparencia del sistema financiero. En el contexto de las instituciones bancarias, las cuentas corrientes y de ahorro se han convertido en canales recurrentes para movilizar fondos de origen ilícito, lo que representa un desafío constante para los mecanismos tradicionales de supervisión. Esta situación se agrava en un entorno digitalizado, donde el volumen y la velocidad de las transacciones dificultan la detección oportuna de operaciones sospechosas mediante métodos convencionales.

En el Perú, la Superintendencia de Banca, Seguros y AFP (SBS) ha reportado un crecimiento sostenido en los Reportes de Operaciones Sospechosas (ROS), alcanzando más de 54 mil reportes entre 2013 y 2023, con montos involucrados que superan los 16 mil millones de dólares. Este panorama evidencia la necesidad urgente de adoptar soluciones tecnológicas más eficaces, que permitan a las entidades financieras anticiparse a los riesgos y cumplir con los estándares regulatorios nacionales e internacionales.

En este contexto, la presente investigación propone el desarrollo de un modelo predictivo basado en técnicas de aprendizaje automático para la detección temprana de transacciones sospechosas de lavado de activos. Para ello, se emplea el simulador AMLSim de IBM, que permite generar datos sintéticos representativos de transacciones bancarias reales, facilitando la experimentación y evaluación de distintos algoritmos de clasificación. El estudio se enmarca en un tipo aplicativo, de nivel explicativo y diseño cuasi-experimental, y evalúa siete modelos de aprendizaje automático: Regresión Logística, SVM, KNN, ANN, Árbol de Decisión, Random Forest y XGBoost.

La importancia de esta investigación radica en su contribución teórica, metodológica y práctica. Teóricamente, amplía el conocimiento sobre la aplicación de inteligencia artificial en la prevención del lavado de activos. Metodológicamente, establece un

marco replicable para la implementación de modelos predictivos en entornos bancarios. Y en el plano práctico, ofrece una herramienta que puede fortalecer los sistemas de monitoreo y reducir los riesgos operativos y reputacionales de las entidades financieras.

La tesis se estructura en cinco capítulos. El primer capítulo presenta las generalidades, la realidad problemática, la formulación del problema, la justificación del estudio, hipótesis, objetivos y limitantes del estudio. El segundo capítulo desarrolla el marco teórico y conceptual, incluyendo antecedentes nacionales e internacionales, así como las bases teóricas de la variable dependiente e independiente y el marco conceptual del lavado de activos y del aprendizaje automático. El tercer capítulo describe el método de la investigación, detallando el tipo, nivel, diseño y enfoque de la investigación, la población y muestra, las variables, y la técnica e instrumentos de recolección y método de análisis de datos. El cuarto capítulo expone el desarrollo del trabajo de investigación, se explica paso a paso la solución. En el quinto capítulo se desarrolla el análisis y discusión de los resultados descriptivos e inferenciales Finalmente se presentan las conclusiones y recomendaciones para futuras investigaciones y aplicaciones prácticas.

CAPÍTULO I

PARTE INTRODUCTORIA DE LA TESIS

1.1 GENERALIDADES

La empresa IBM ha desarrollado un simulador de agentes múltiples que es único en su tipo, por lo que ha publicado el proyecto AMLSim bajo una licencia de código abierto (Suzumura & Kanezashi, 2021). Esto significa que cualquier persona puede utilizar el simulador, lo que contribuye a la difusión del conocimiento y la colaboración en la lucha contra el lavado de dinero. El simulador es capaz de generar datos sintéticos de transacciones bancarias que son realistas y representativos de la actividad real. Esto permite a los investigadores probar y evaluar nuevos algoritmos de detección de lavado de dinero de una manera más precisa y eficaz.

En definitiva, el proyecto AMLSim se erige como una herramienta esencial para combatir el lavado de dinero al permitir a la presente investigación evaluar algoritmos y mejorar la eficacia de los sistemas de detección de una entidad bancaria, por lo que este simulador juega un papel crucial en la lucha contra las actividades financieras ilícitas.

1.2 REALIDAD PROBLEMÁTICA

El lavado de activos representa una amenaza significativa para la integridad y estabilidad del sistema financiero en la actualidad (GAFILAT, 2017). En el contexto de las instituciones bancarias, las cuentas corrientes y de ahorros se han convertido en vehículos preferidos para llevar a cabo actividades ilegales y fraudulentas. Los métodos tradicionales de monitoreo y detección de transacciones sospechosas se han vuelto insuficientes en la era

digital y altamente tecnológica en la que nos encontramos. En este sentido, las organizaciones financieras, se enfrentan al desafío crítico de desarrollar sistemas de vigilancia avanzados que no solo sean capaces de identificar patrones complejos y sutiles asociados con el lavado de activos, sino también de hacerlo de manera temprana y precisa para prevenir eficazmente estas actividades ilícitas.

Este problema se vuelve aún más crítico dado el contexto en el que se lleva a cabo este estudio para entidades bancarias. La necesidad de implementar soluciones prácticas y efectivas es urgente, ya que el fracaso en detectar y prevenir estas actividades ilegales puede no solo resultar en pérdidas financieras significativas para el banco, sino también en daños reputacionales irreparables y posibles consecuencias legales. Por lo tanto, este estudio se convierte en un esfuerzo vital para fortalecer las defensas del banco contra el lavado de activos, asegurando así la confianza de los clientes, cumpliendo con las regulaciones gubernamentales y fortaleciendo la integridad del sistema financiero en su conjunto.

Según el FMI (2018) estima que entre el 2% y 5% del PBI mundial se lava cada año, lo que equivale a entre USD 1.6 y 4 billones. Según la UNODC (2022) advierte que solo una pequeña fracción de este dinero es finalmente detectada y recuperada. Además, según GAFILAT (2017) señala que en Latinoamérica el uso de efectivo, los negocios informales y la corrupción agravan la vulnerabilidad frente al lavado

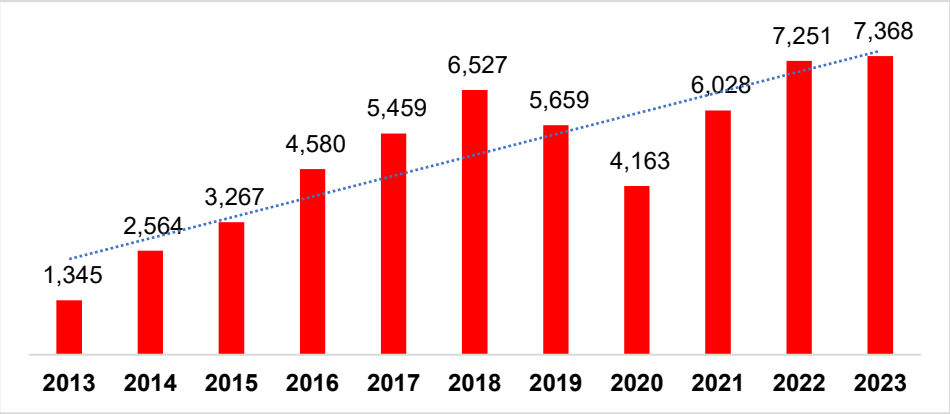
En la Figura 1 se muestra que, a nivel nacional, la Superintendencia de Banca, Seguros y AFP (SBS, 2023) consolida los Reportes de Operaciones Sospechosas (ROS) generados por las entidades sujetas a su supervisión. Entre los años 2013 y 2023, se registró un total acumulado de 54,211 reportes, con un monto involucrado que asciende a USD 16,158 millones, como se evidencia en la Figura 2. Durante este periodo, la cantidad de ROS ha mantenido una tendencia creciente, con un promedio de crecimiento anual del 22 %. El incremento más significativo se produjo entre 2017 y 2018, con una variación de 19.57 %, atribuida principalmente al aumento en los reportes provenientes de empresas de transferencias de fondos. En cuanto a los

montos económicos asociados a los ROS, se observa un crecimiento promedio anual del 49 %, destacando el año 2018 como el de mayor volumen reportado, con un total de USD 3,370 millones.

Cabe mencionar que la señal de alerta más reportada e identificada por el sector de Bancos es “El cliente se niega a proporcionar la información solicitada o la información proporcionada es inconsistente o de difícil verificación por parte de las empresas”. En sí misma esta señal puede o no confirmar directamente la detección por lavado de activos.

Figura 1

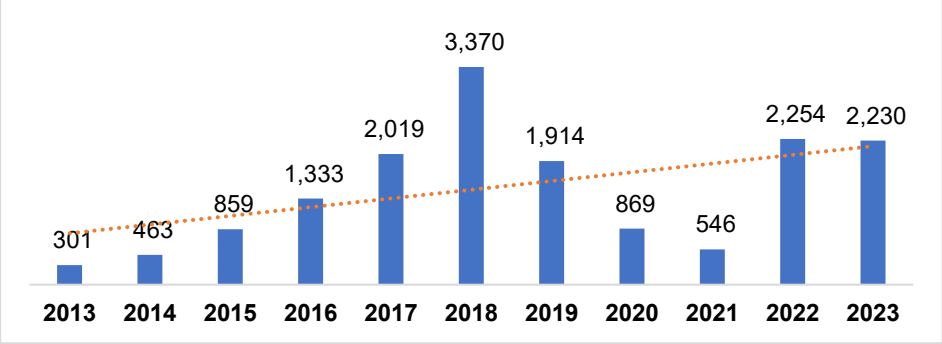
Cantidad de ROS recibidos anualmente (2013-2023)



Nota. Tomado de los Reportes de Operaciones Sospechosas por la SBS 2023.

Figura 2

Monto en millones de USD de los ROS recibidos anualmente (2013-2023)



Nota. Tomado de los Reportes de Operaciones Sospechosas por la SBS 2023

En consecuencia, esta investigación se centra en el desarrollo y evaluación de un modelo predictivo de Aprendizaje automático que no solo sea capaz de identificar patrones sospechosos de manera temprana, sino que también se adapte y evolucione continuamente para enfrentar las cambiantes tácticas y estrategias utilizadas por los delincuentes financieros. Resolver este problema no solo implica mejorar la eficiencia operativa del banco, sino que también contribuirá significativamente a la lucha global contra el lavado de activos, promoviendo así la transparencia y la integridad en el sistema financiero.

1.3 FORMULACIÓN DEL PROBLEMA

En este contexto, el problema principal que se abordará en esta tesis radica en la necesidad imperante de identificar y emplear el mejor modelo de Aprendizaje automático para la detección temprana y precisa de transacciones sospechosas en cuentas bancarias, específicamente relacionadas con el lavado de activos. De acuerdo con ello se establece el problema general y problemas específicos.

1.3.1 Problema general

PG: ¿Cómo influye la implementación de un modelo predictivo de aprendizaje automático en la detección temprana de transacciones de lavado de activos en entidades financieras?

1.3.2 Problemas específicos:

PE1: ¿Cómo influye la implementación del modelo predictivo seleccionado en la sensibilidad (Recall) para la detección temprana de transacciones de lavado de activos en entidades financieras?

PE2: ¿Cómo influye la implementación del modelo predictivo seleccionado en la precisión (Precision) para la detección temprana de transacciones de lavado de activos en entidades financieras?

PE3: ¿Cómo influye la implementación del modelo predictivo seleccionado en el área bajo la curva ROC (AUC-ROC) para la detección temprana de transacciones de lavado de activos en entidades financieras?

1.4 JUSTIFICACIÓN DEL ESTUDIO

1.4.1 Teórica

La investigación tiene una relevancia teórica significativa al contribuir al avance del conocimiento en el campo del lavado de activos y la aplicación de modelos de Aprendizaje automático en el sector bancario. Al desarrollar y evaluar un modelo predictivo específico para la detección temprana de operaciones sospechosas en cuentas bancarias, se ampliará la comprensión de cómo las técnicas de Aprendizaje automático pueden ser adaptadas y aplicadas de manera efectiva en un contexto bancario real. Esto permitirá la construcción de nuevas teorías y conceptos relacionados con la prevención del lavado de activos mediante enfoques tecnológicos innovadores (Blanco-Cordero et al., 2014).

1.4.2 Metodológica

La investigación tiene una importancia metodológica al demostrar la aplicación práctica de técnicas de Aprendizaje automático en un entorno bancario específico. Al desarrollar un modelo predictivo, se establecerán metodologías y mejores prácticas para la implementación exitosa de algoritmos de Aprendizaje automático en la detección de actividades sospechosas. Los métodos y enfoques desarrollados en esta investigación podrán servir como guía para futuros estudios en el campo de la seguridad financiera y la prevención del lavado de activos, proporcionando un marco metodológico sólido para investigaciones similares (Barbosa-Moreno et al., 2020).

1.4.3 Práctica

La investigación tiene una relevancia práctica directa para una entidad bancaria. Al desarrollar un modelo de detección temprana y precisa de

operaciones sospechosas, un banco estará mejor equipado para prevenir el lavado de activos y proteger sus activos y reputación. La implementación exitosa de este modelo tendrá un impacto directo en las operaciones diarias de un banco, mejorando la eficacia de los sistemas de seguridad y cumpliendo con las regulaciones gubernamentales y de la industria. Además, al aumentar la capacidad del banco para identificar y prevenir actividades ilícitas, se fortalecerá la confianza de los clientes y se mejorará la integridad de un banco en el mercado financiero (Barbosa-Moreno et al., 2020).

1.5 HIPÓTESIS

La detección de transacciones sospechosas en cuentas bancarias se ha convertido en una herramienta esencial, requiriendo técnicas avanzadas de análisis de datos y modelos predictivos. Los estudios previos realizados por Singh & Best (2019) y Lokanan (2024) destacan la importancia de utilizar técnicas analíticas y modelos de aprendizaje automático para detectar y prevenir el lavado de dinero en el sector bancario.

Frente a lo expuesto, se sostiene la siguiente hipótesis general e hipótesis específicos.

1.5.1 Hipótesis general

HG: La implementación de un modelo predictivo de aprendizaje automático mejora en la detección temprana de transacciones de lavado de activos en entidades financieras.

1.5.2 Hipótesis específicas

HE1: La implementación del modelo predictivo seleccionado influye positivamente en el incremento de la sensibilidad (Recall) en la detección temprana de transacciones de lavado de activos en entidades financieras.

HE2: La implementación del modelo predictivo seleccionado influye positivamente en el incremento de precisión (Precision) en la detección temprana de transacciones de lavado de activos en entidades financieras.

HE3: La implementación del modelo predictivo seleccionado influye positivamente en el incremento del área bajo la curva ROC (AUC-ROC) en la detección temprana de transacciones de lavado de activos en entidades financieras.

1.6 OBJETIVOS

El lavado de activos es una preocupación global que afecta a la integridad y estabilidad del sistema financiero (Fernández-Murillo et al., 2022). Por lo cual es considerado como un proceso mediante el cual los delincuentes transforman fondos obtenidos de actividades ilícitas en apariencia de fondos legítimos (Kaur, 2019). En esa misma línea, Kumar (2015) argumenta que esto les permite ocultar el origen y la propiedad de dichos activos, evadir el alcance de las autoridades y utilizarlos para financiar otras actividades criminales o para legitimarlos en la economía legal.

Dado el alcance y la gravedad de este problema, resulta fundamental desarrollar mecanismos efectivos para detectar y prevenir el lavado de activos (Ghulam & Szalay, 2024). En este sentido, la detección de transacciones sospechosas en cuentas bancarias se ha convertido en una herramienta esencial para las instituciones financieras y las autoridades reguladoras (Hassan et al., 2023).

Chen et al. (2018) sostiene que la detección de transacciones sospechosas en cuentas bancarias implica el análisis y monitoreo de las actividades financieras de los clientes, con el fin de identificar patrones y comportamientos que puedan indicar la existencia de actividades ilícitas. Para lograr esto, se requiere el uso de técnicas avanzadas de análisis de datos y modelos predictivos, que permitan identificar anomalías y generar alertas tempranas (Singh & Best, 2019).

Varios autores han investigado y propuesto enfoques y metodologías para la detección de transacciones sospechosas relacionadas con el lavado de activos. Por ejemplo, en el estudio de Singh & Best (2019), se destaca la importancia de utilizar técnicas de aplicación del análisis de enlaces para visualizar las transacciones bancarias que afectan a una entidad y con ello

ayudar en la detección de transacciones y actividades potencialmente relacionadas con el lavado de dinero. Frente a lo expuesto, se sostiene el siguiente objetivo general y objetivos específicos.

1.6.1 Objetivo General

OG: Determinar la influencia de la implementación de un modelo predictivo de aprendizaje automático en la detección temprana de transacciones de lavado de activos en entidades financieras.

1.6.2 Objetivos específicos

OE1: Determinar la influencia de la implementación del modelo predictivo seleccionado sobre la sensibilidad (Recall) en la detección temprana de transacciones de lavado de activos en entidades financieras.

OE2: Determinar la influencia de la implementación del modelo predictivo seleccionado sobre la precisión (Precision) en la detección temprana de transacciones de lavado de activos en entidades financieras.

OE3: Determinar la influencia de la implementación del modelo predictivo seleccionado sobre el área bajo la curva ROC (AUC-ROC) en la detección temprana de transacciones de lavado de activos en entidades financieras.

1.7 LIMITANTES DE LA INVESTIGACIÓN

1.7.1 Limitante temporal

La investigación estará delimitada temporalmente al período de la última actualización que se realizó a la fuente de datos. Esta delimitación se justifica por la necesidad de utilizar datos recientes y relevantes para desarrollar y evaluar el modelo de Aprendizaje automático. Al enfocarse en este marco temporal, se asegura que los datos utilizados sean representativos de las tendencias y patrones actuales en las transacciones financieras y actividades de lavado de activos (Quintero-Acuña, 2023).

1.7.2 Limitante espacial

La investigación se llevará a cabo a partir de las transacciones simuladas al de una entidad bancaria. Las observaciones, recopilación de datos y pruebas del modelo estarán limitadas a las transacciones realizadas en las cuentas gestionadas y generadas por el proyecto AMLSim, lo que facilita diversas aplicaciones, incluida la detección de fraude y/o actividades sospechosas. Esta delimitación garantiza un enfoque específico y centrado en el contexto bancario (Useche et al., 2019).

1.7.3 Limitante de recursos

Los recursos disponibles para la investigación estarán limitados a los datos del proyecto AMLSim, mientras que los recursos computacionales y humanos serán proporcionados por el investigador del presente estudio. Se utilizarán herramientas de software y hardware disponibles para el desarrollo, entrenamiento y evaluación del modelo de aprendizaje automático (Manrique-Rojas, 2020).

Esta delimitación implica que no se tendrán en cuenta otros recursos que podrían estar disponibles fuera del proyecto AMLSim, como bases de datos externas. Además, se reconoce que, debido a restricciones de tiempo y recursos, la investigación no podrá abordar todos los posibles algoritmos y enfoques de Aprendizaje automático existentes, sino que se centrará en aquellos considerados más prometedores y adecuados para el contexto específico de una entidad bancaria.

CAPÍTULO II

MARCO TEÓRICO Y CONCEPTUAL

2.1 ANTECEDENTES DE INVESTIGACIÓN

2.1.1 Antecedentes internacionales

En el ámbito internacional, en el trabajo de investigación de Gracia (2016), en Colombia, busco proponer un modelo de detección de operaciones sospechosas de lavado de activos que puedan ayudar a reducir las tasas de falsos positivos incorporando tanto variables transaccionales convencionales como las no convencionales para obtener los mejores indicadores en el modelo creado, en ese sentido se comparó los distintos modelos de detección como: red bayesiana dinámica, red neuronal de base radial, máquina de soporte vectorial, clúster de dos fases, esperanza – maximización y sequence matching. Dónde a partir de todos los modelos implementados el que obtiene los mejores resultados y puede ser la técnica base a partir del cual se construya un nuevo modelo para la detección de actividades sospechosas es SVM (máquina de soporte vectorial). En conclusión, se destaca la eficacia de este modelo para futuras investigaciones en este ámbito financiero.

En este estudio se destaca la importancia de incorporar tanto variables transaccionales convencionales como no convencionales en la detección de lavado de activos. Además, resalta la eficacia del modelo de máquina de soporte vectorial (SVM) en la detección de operaciones sospechosas. Estos hallazgos pueden ser útiles para futuras investigaciones y contribuir al desarrollo de estrategias y modelos más efectivos en la detección de actividades ilícitas en el ámbito financiero.

En tanto, en el estudio de Quishpe (2022) desarrolló e implemento modelos de segmentación de clientes basados en Aprendizaje automático para detectar riesgos de lavados de activos y financiación del terrorismo (LAFT), para el caso de estudio de una aseguradora. En ese marco la segmentación fue aplicada para personas naturales y jurídicas con la finalidad de determinar el grupo de clientes con mayor riesgo LAFT identificando así las transacciones sospechosas de estos grupos con alto riesgo y tomar acciones a través de alertas que fueron aplicadas en el desarrollo del modelo propuesto. A partir de las variables utilizadas en el modelo se hacen cuatro segmentaciones para las personas jurídicas y cinco segmentaciones para las personas naturales, usando del índice de Dunn, garantizando la homogeneidad y heterogeneidad en los segmentos, en ese sentido también se usó la técnica de Análisis de Componentes Principales (ACP), posteriormente para el apartado de clasificación de los datos se implementó el modelo de Random Forest en los dos factores de riesgo tanto personas naturales y jurídicas. En conclusión, la construcción de los modelos se hizo en dos etapas usando en una primera instancia los modelos no supervisados para agrupar los segmentos y en la segunda con las etiquetas para evaluar en cada caso los modelos supervisados, permitiendo lograr con efectividad el control adecuado de las actividades ilícitas de las entidades financieras en el comportamiento de clientes que presentan un mayor riesgo LAFT.

Este estudio contribuye al desarrollo de modelos de segmentación de clientes basados en aprendizaje automático para detectar riesgos de LAFT. Estos modelos permiten identificar y controlar de manera efectiva las actividades ilícitas en el comportamiento de los clientes, brindando a las entidades financieras herramientas importantes para la prevención y mitigación de riesgos relacionados con el lavado de activos y la financiación del terrorismo.

Por otro lado, Němec (2019) en su trabajo titulado "Aprendizaje automático for financial crime detection" investigó técnicas de minería de datos que pueden ser utilizadas para detectar delitos financieros para luego proponer e implementar un modelo de Aprendizaje automático para este

problema basado en la información obtenida. En ese contexto se usaron varios modelos, en primer lugar, se utilizó un modelo base basado en un algoritmo de árbol de decisión. Este modelo base fue evaluado para medir su rendimiento en la detección de entidades fraudulentas. Posteriormente, se propusieron mejoras al modelo base, como la introducción de la sensibilidad al costo y el uso de un conjunto de datos de entrenamiento ponderado. Estas mejoras se implementaron utilizando el algoritmo AdaCost, que es un algoritmo de ensamblaje sensible al costo. El modelo mejorado fue evaluado para medir su rendimiento y su capacidad de reducir el número de falsos positivos. Además, se llevó a cabo una comparación entre todos los modelos implementados, incluyendo el modelo base y el modelo mejorado, para determinar cuál de ellos ofrecía el mejor rendimiento en términos de detección de delitos financieros. En conclusión, se logra implementar varios modelos, incluyendo un modelo base basado en un algoritmo de árbol de decisión y un modelo mejorado utilizando el algoritmo AdaCost. Estos modelos al ser evaluados y comparados muestran mejoras en el rendimiento del modelo base al reducir los falsos positivos, por lo tanto, estos modelos de Aprendizaje automático ayudan a la detección oportuna de delitos financieros.

En ese sentido, el estudio demuestra que la aplicación de técnicas de aprendizaje automático, como el algoritmo AdaCost, puede ayudar a mejorar la detección de delitos financieros al reducir los falsos positivos y proporcionar detección oportuna. Esto tiene implicaciones importantes para la prevención y combate de actividades delictivas en el ámbito financiero.

Por último, tenemos que el estudio de Cortés-Sánchez (2023) que tuvo como objetivo establecer alternativas metodológicas robustas que permitan dar cumplimiento del Anti Money Laundering (AML), “Prevención de Lavado de Dinero”, a partir de la implementación de técnicas de Aprendizaje automático con la finalidad de dar confianza y lealtad a los clientes, asimismo de buscar eficiencias y garantizando la buena reputación de una entidad financiera. En cuanto a los modelos analíticos se propone la implementación de múltiples técnicas de Aprendizaje automático, específicamente de aprendizaje no supervisado, para la detección de transacciones anómalas,

utilizando técnicas como el Grafo Transaccional que captura la estructura de las interacciones de los clientes con la magnitud de sus transacciones, posteriormente a ello se usó el algoritmo Node2vec, para capturar mucho mejor las relaciones en un grafo en un espacio con menor dimensionalidad, luego se propuso la Detección de Anomalías dónde se usaron tres algoritmos: Isolation Forest, Histogram Based Outlier (HBOS) y Angle-Based Outlier Detection (ABOD) para identificar los patrones de las transacciones que se desvían, por otro lado, se aplicó los PCA Anomaly Scores para reducir la dimensionalidad del gran volumen de datos y delimitar las puntuaciones anómalas. Los resultados obtenidos muestran la efectividad de cada una de las metodologías propuestas en la identificación de transacciones y la caracterización de los individuos involucrados en estas transacciones. Además, se logra una disminución significativa en la carga operativa en actividades de investigación de AML.

El aporte principal de este estudio es presentar y validar un conjunto de técnicas de Aprendizaje Automático para mejorar la detección de transacciones anómalas y fortalecer la prevención de lavado de dinero en entidades financieras. Los resultados obtenidos demuestran la efectividad de estas técnicas y su potencial para reducir la carga operativa en la investigación de actividades sospechosas de lavado de dinero.

2.1.2 Antecedentes nacionales

En el ámbito de Perú, el trabajo de investigación que propuso Molina-Salvador (2016) fue el emplear el análisis clúster de K-Medias como una metodología innovadora para segmentar a los clientes (personas naturales) en clústeres según su comportamiento operacional con la finalidad de detectar las actividades sospechosas por lavado de activos. Posteriormente, se identificarán los casos atípicos basándose en distancias y se utilizó la técnica CHAID para clasificar a los clientes en un clúster operacional. Esta estrategia comprehensiva buscó no solo categorizar a los clientes en grupos operacionales, sino también detectar patrones inusuales y comportamientos atípicos, mejorando significativamente la capacidad de prevención del lavado

de activos en el sector del mercado de valores. En conclusión, el impacto de esta metodología implementada a partir de los modelos se traduce en una significativa mejora en la capacidad de prevención del lavado de activos en el sector financiero.

El aporte principal de este estudio destaca en la importancia de utilizar el análisis clúster de K-Medias y técnicas adicionales como la detección de casos atípicos y CHAID para mejorar la capacidad de prevención del lavado de activos en el sector del mercado de valores. Esta metodología proporciona una visión más completa y precisa de los comportamientos de los clientes, lo que facilita la detección temprana de actividades sospechosas y contribuye a la seguridad y transparencia del sector financiero.

Por otro lado, en el estudio de Ezcurra-Silva (2016) se enfocó en cumplir con las estrictas regulaciones establecidas por la Superintendencia del Mercado de Valores (SMV) para las sociedades titulizadoras en Perú, específicamente en lo que respecta a la prevención del lavado de activos y financiamiento del terrorismo (SPLAFT). Siguiendo un enfoque basado en riesgos (EBR) y en consonancia con el Plan nacional de lucha contra el lavado de activos y financiamiento del terrorismo, adoptó una metodología de gestión de riesgos paso a paso. Este enfoque implicó la evaluación meticulosa de los eventos de riesgo clave, el cálculo tanto del riesgo inherente como del riesgo residual, el diseño de controles efectivos y la evaluación del impacto de estos controles. En conclusión, dicha guía, se basa en las directrices del Grupo de Acción Financiera Internacional (GAFI) e incorpora la metodología basada en riesgos (EBR) para abordar las cuestiones relacionadas con la prevención del lavado de activos y financiamiento al terrorismo.

Por lo tanto, esta indagación proporciona una guía y metodología basada en riesgos para abordar las cuestiones relacionadas con la prevención del lavado de activos y financiamiento del terrorismo en las sociedades titulizadoras en Perú. Este enfoque permite identificar y gestionar los riesgos de manera efectiva, cumpliendo con las regulaciones establecidas por la SMV y siguiendo las directrices internacionales del GAFI.

Mientras que el estudio de Galeano-Villar & Vargas-Cisneros (2019) proponen como objetivo identificar modelos de aprendizaje automático que han sido implementados para el apoyo en la detección de transacciones sospechosas de lavado de activos en entidades financieras. En ese marco los autores buscan analizar la metodología sistémica detrás de los modelos utilizados a partir de la literatura consultada de 485 publicaciones, donde el 77% son artículos de tipo Journal y el 23% artículos de conferencia. En cuanto a los principales resultados que se llegó a partir de los artículos seleccionados es que los 5 métodos de aprendizaje automático más usados en este tipo de casuística son el modelo de Zengan, modelo de Tang y Yin, modelo de Liu Zhang, modelo de Luna, Palshikar, Apte, y Bhattacharya, y por último, el modelo de Larik y Haider, cada uno de estos fueron empleados para la detección del campo de acción del delito. Cabe destacar que el algoritmo SVM es uno de los que se utilizan en los diferentes modelos propuestos, por otro lado, otros algoritmos que tienen relevancia en el ámbito de estudio son los Decision Tree y el Random Forest. En conclusión, estos modelos de aprendizaje automático requieren de una exactitud de un 90% a 95%, para que sean efectivos y determinar los casos sospechosos de lavado de activos, además cabe destacar que muchos de los modelos están basados en algoritmos de clustering como punto de partida debido a que se necesita realizar previamente cierta agrupación a los clientes, cuentas y transacciones.

El aporte de este estudio proporciona una visión general de los modelos de aprendizaje automático utilizados en la detección de lavado de activos en entidades financieras. Identifica los métodos más utilizados, destaca la importancia de algoritmos como SVM, Decision Tree y Random Forest, y resalta el papel de los algoritmos de clustering en la segmentación de datos para una detección más precisa. Además, estos hallazgos contribuyen al campo de la prevención y detección de lavado de activos en el sector financiero.

Finalmente, en el trabajo de investigación de Rodríguez-Mallma (2022) propone implementar un modelo que permita identificar a los clientes con riesgo de operaciones sospechosas, basado en cinco fases: entender el

problema de negocio, preparar los datos, construir el modelo, análisis de errores e integrar el modelo a un sistema. En cuanto a la implementación de los algoritmos de Aprendizaje automático, usó las siguientes técnicas: Random Forest, XGBOOST, y el LGBM, dónde los compara y demuestra que los modelos de gradiente boosting son los que poseen métricas similares en las etapas del TRAIN y TEST, además el modelo que destaca por su performance es el LGBM debido a que presenta menor diferencia en estas dos etapas lo que se traduce que se comporta de manera parecida asimismo de que tiene muy buenos indicadores, además este modelo en particular posee un bajo consumo en recursos computacionales. En conclusión, a partir de las métricas de los modelos considerados permiten discriminar mejor a los clientes con actividades sospechosas en una entidad bancaria.

Esta indagación aporta al campo de la identificación de clientes con riesgo de operaciones sospechosas en entidades bancarias mediante la implementación de un modelo de aprendizaje automático. Su metodología de cinco fases proporciona una estructura clara para el desarrollo del modelo, y la comparación de algoritmos demuestra que los modelos de gradiente boosting, especialmente el LGBM, muestran un buen desempeño en términos de métricas y consumo de recursos. Esto permite una mejor discriminación de los clientes con actividades sospechosas, contribuyendo así a la prevención y detección de actividades ilícitas en el ámbito bancario.

2.2 BASES TEÓRICAS

2.2.1 Variable Dependiente: Detección de transacciones de lavado de activos

Según el Grupo de Acción Financiera Internacional (GAFI, 2020), el lavado de activos permite ocultar o disimular el origen de ganancias obtenidas mediante actividades ilegales, representando una amenaza directa para la integridad del sistema financiero.

Ante esta problemática, la “detección de transacciones de lavado de activos” se refiere al proceso mediante el cual las instituciones financieras y otras entidades relevantes identifican y analizan transacciones que presentan características sospechosas o inusuales, con el objetivo de prevenir y combatir el lavado de dinero y el financiamiento del terrorismo. Este proceso implica el uso de técnicas analíticas, algoritmos de aprendizaje automático y sistemas de monitoreo en tiempo real para identificar patrones de comportamiento que puedan indicar actividades ilícitas

a. Transacciones Sospechosas de Lavado de Activos

Las transacciones sospechosas de lavado de activos son operaciones financieras que, debido a su naturaleza, monto, frecuencia, complejidad o contexto, generan dudas razonables sobre la legitimidad de los fondos involucrados. Estas operaciones pueden no contar con un propósito económico o legal aparente y, en muchos casos, podrían estar diseñadas para ocultar el origen ilícito del dinero, dificultando su detección dentro del sistema financiero.

De acuerdo con el Grupo de Acción Financiera Internacional (GAFI, 2020), las instituciones financieras están obligadas a identificar y reportar transacciones sospechosas que pudieran estar relacionadas con el lavado de activos o el financiamiento del terrorismo. Para ello, deben considerar factores como la naturaleza inusual de la transacción, el perfil del cliente y el contexto operativo en el que se realiza.

En la misma línea, el Banco Mundial (2019) sostiene que las transacciones sospechosas son aquellas que, por su monto, frecuencia o tipo de operación, no se alinean con el comportamiento económico habitual del cliente ni con su actividad declarada, lo cual puede ser indicio de un intento de ocultamiento de fondos de origen ilícito.

Estas definiciones coinciden con lo establecido por la Superintendencia de Banca, Seguros y AFP (SBS, 2015) en el marco legal peruano, donde se describe a las operaciones sospechosas como aquellas inusuales, sin justificación económica o legal aparente, y que resulten incompatibles con el

perfil del cliente, debiendo ser reportadas a la Unidad de Inteligencia Financiera (UIF) en un plazo máximo de 24 horas.

b. Importancia de la Detección Temprana

La detección temprana de estas operaciones es fundamental para prevenir que los fondos ilícitos completen el ciclo de lavado y se integren plenamente a la economía formal. Según Ngai et al. (2011), identificar estos patrones a tiempo:

- Minimiza los riesgos reputacionales y legales de las instituciones.
- Facilita la cooperación con la Unidad de Inteligencia Financiera (UIF).
- Cumple con las normativas nacionales como la Ley N° 27693 en Perú.

Además, una detección eficaz fortalece la confianza en el sistema financiero y contribuye a la transparencia de los mercados.

c. Etapas del Lavado de Activos

De acuerdo con la GAFI (2020) y la UNODC (2022), el proceso de lavado de activos se compone de tres etapas:

- **Colocación**

La colación es una de las fases del proceso de lavado de activos, también conocido como blanqueo de capitales. Esta etapa implica la introducción de los fondos ilícitos en el sistema financiero o económico de manera gradual y disimulada, con el objetivo de dificultar su rastreo y ocultar su origen ilícito (Palombini, 2021).

Lucero-Chunir & Sánchez-Gutiérrez (2023) mencionan que, durante la colocación en etapas, los delincuentes buscan distribuir los fondos ilícitos en diferentes cuentas bancarias, inversiones o transacciones comerciales para evitar levantar sospechas y evitar la detección por parte de las autoridades. Esta fase puede involucrar el uso de intermediarios, empresas ficticias o transacciones internacionales complejas para complicar aún más el seguimiento del dinero.

El propósito principal de la colocación en etapas es integrar los fondos ilícitos en el sistema financiero de manera que parezcan legítimos (Santillán-Molina et al., 2022). Una vez que los fondos se han colocado en diferentes

cuentas o inversiones, el siguiente paso en el proceso de lavado de activos involucra su estratificación o superposición, que implica realizar transacciones adicionales para ocultar aún más el origen de los fondos.

- **Estratificación**

La estratificación implica la realización de múltiples transacciones financieras o comerciales complejas con el fin de dificultar aún más el rastreo del origen ilícito de los fondos. Durante esta etapa, los delincuentes buscan ocultar y mezclar los fondos ilícitos mediante la realización de transferencias entre cuentas, inversiones, compras y ventas de activos, o cualquier otra actividad que les permita dar la apariencia de que los fondos tienen un origen legítimo (Palombini, 2021).

Lucero-Chunir & Sánchez-Gutiérrez (2023) sostienen que el objetivo de la estratificación es complicar el seguimiento del dinero y dificultar la identificación de su fuente ilícita. Los delincuentes pueden utilizar múltiples intermediarios, transacciones internacionales, empresas ficticias y otros métodos para confundir a las autoridades y dificultar la detección del origen ilegal de los fondos.

- **Integración**

La integración es la tercera y última fase del proceso de lavado de activos, también conocido como blanqueo de capitales. Esta etapa se refiere al proceso de reintroducir los fondos ilícitos ya lavados en la economía legal de manera que parezcan legítimos y no levanten sospechas (Palombini, 2021).

Durante la integración en etapas, los delincuentes buscan incorporar los fondos ilícitos en actividades económicas legales, como inversiones en bienes raíces, adquisición de empresas, creación de negocios legítimos u otras inversiones financieras. El objetivo es convertir los fondos ilícitos en activos aparentemente legales y que puedan ser utilizados sin levantar sospechas por parte de las autoridades o instituciones financieras (Lucero-Chunir & Sánchez-Gutiérrez, 2023).

Esta fase del proceso de lavado de activos implica una variedad de métodos y mecanismos para dar la apariencia de que los fondos tienen un

origen legítimo. Puede incluir la compra de propiedades, inversiones en el mercado de valores, apertura de negocios, realización de transacciones comerciales legítimas, entre otros (Santillán-Molina et al., 2022).

La integración en etapas busca diluir y mezclar los fondos ilícitos con los flujos financieros legales, de manera que sea difícil rastrear su origen ilegal. Esto permite a los delincuentes disfrutar y utilizar los fondos sin levantar sospechas y sin poner en riesgo la detección de sus actividades ilícitas.

d. Enfoques Tradicionales y Modernos en la Detección

Inicialmente, la detección de lavado de activos se realizaba mediante reglas estáticas y umbrales predefinidos. Sin embargo, como advierten Phua et al. (2010), estos métodos presentan limitaciones como:

- Alta generación de falsos positivos.
- Poca adaptabilidad ante nuevas tipologías delictivas.
- Incapacidad de procesar grandes volúmenes de datos.

Ante ello, se han incorporado técnicas de minería de datos y aprendizaje automático, que permiten detectar patrones ocultos y dinámicos en grandes bases de datos (Ngai et al., 2011)

Beneficios del Aprendizaje Automático en la Detección: El machine learning ha demostrado ser efectivo para enfrentar estos desafíos. Según Ngai et al. (2011), algoritmos como XGBoost, Random Forest, Support Vector Machine (SVM) y Redes Neuronales permiten:

- Procesar datos en tiempo real.
- Reducir los falsos positivos.
- Adaptarse a patrones delictivos emergentes.

Zhang & Trubey (2019) destacan que el aprendizaje automático optimiza la priorización de alertas, facilitando la labor de los analistas y reforzando la prevención de delitos financieros.

e. Dimensiones e Indicadores

En esta investigación, la variable dependiente corresponde a la detección de transacciones de lavado de activos. Para evaluarla de manera integral, se han definido tres dimensiones que permiten medir el rendimiento

de los modelos predictivos aplicados. Cada dimensión está asociada a un indicador específico, el cual es ampliamente utilizado en la evaluación de modelos de clasificación binaria, especialmente en problemas donde existe un desbalance entre clases, como es el caso de lavado de activos.

- **Efectividad en la clasificación:** Esta dimensión evalúa la capacidad del modelo para identificar correctamente las transacciones realmente sospechosas dentro del conjunto de datos. Es especialmente relevante en la lucha contra el lavado de activos, que un bajo desempeño en esta dimensión podría permitir que transacciones ilícitas pasen desapercibidas.
    - **Sensibilidad o Recall:** Esta métrica es el indicador de la dimensión mencionada en el anterior párrafo, mide la capacidad del modelo para identificar correctamente las transacciones sospechosas. Se calcula dividiendo el número de transacciones sospechosas clasificadas correctamente entre el número total de transacciones sospechosas. Un mayor recall indica que el modelo puede identificar de manera más efectiva las transacciones sospechosas (Nayyer et al., 2023). La siguiente ecuación 1 representa este indicador:

$$\boldsymbol{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}} \qquad \textbf{(1)}$$

Donde:

$\boldsymbol{TP}$**:** Verdaderos positivos

$\boldsymbol{FN}$: Falsos negativos

- **Precisión en la Clasificación:** La segunda dimensión está enfocada en evaluar la exactitud del modelo al predecir transacciones sospechosas. No basta con detectar muchas; es importante que las que se detecten realmente sean sospechosas.

- **Precisión (Precision):** Esta métrica es el indicador que mide la proporción de transacciones clasificadas correctamente en general, es decir, tanto las transacciones sospechosas como las no sospechosas. Se calcula dividiendo el número total de transacciones clasificadas correctamente entre el número total de transacciones. Una mayor precisión indica un mejor rendimiento general del modelo (Nayyer et al., 2023). La siguiente ecuación 2 representa este indicador:

$$\boldsymbol{Precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FP}} \qquad \textbf{(2)}$$

Donde:

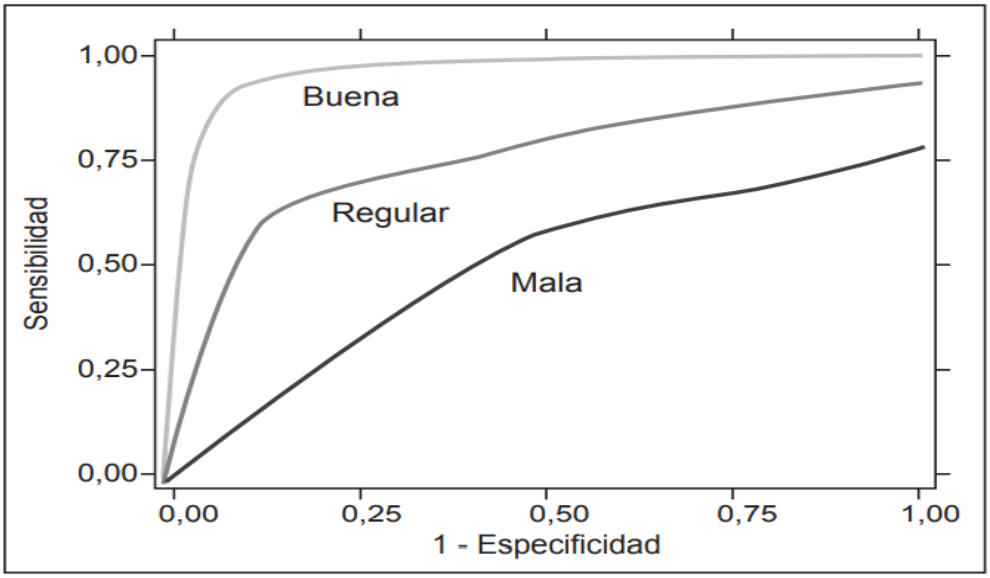
$\boldsymbol{TP}$**:** Verdaderos positivos

$\boldsymbol{FN}$: Falsos positivos

- **Capacidad Discriminativa:** La tercera dimensión busca evaluar el desempeño global del modelo en la diferenciación entre transacciones sospechosas y no sospechosas, sin importar el umbral específico que se use para la clasificación.
    - **Área Bajo la Curva ROC (AUC-ROC):** Esta métrica es el indicador que resume la calidad global del modelo de clasificación. Cuanto mayor sea el valor del AUC-ROC, mejor será el rendimiento del modelo. El AUC-ROC varía entre 0 y 1, donde un valor de 0 indica un rendimiento pobre (clasificación aleatoria) y un valor de 1 indica un rendimiento perfecto (clasificación precisa) (Martínez-Camblor, 2007). En la figura 3 se muestra gráficamente el AUC-ROC.

Figura 3

Esquema explicativo de distintas posibilidades de curvas ROC



Nota. Tomado de Burgos y Manterola (2010).

2.2.2 Variable Independiente: Modelos predictivos de aprendizaje automático

Un modelo predictivo es un tipo de modelo estadístico o computacional que permite estimar la probabilidad de ocurrencia de un evento futuro con base de datos históricos (Shmueli, 2010). Los modelos de aprendizaje automático se han destacado en la detección de transacciones sospechosas debido a sus capacidades para manejar datos complejos, identificar patrones sutiles y adaptarse a diferentes escenarios, proporcionando así una base teórica sólida para el desarrollo del modelo predictivo de esta investigación.

El aprendizaje automático es el campo de estudio que se ocupa de desarrollar algoritmos y modelos que permiten a las computadoras aprender a partir de datos y mejorar su rendimiento en tareas sin ser explícitamente programadas (Mitchell, 1997).

El aprendizaje automático es una rama de la inteligencia artificial que se centra en la creación de sistemas capaces de aprender y mejorar su

desempeño a través de la experiencia, sin necesidad de ser programados de forma explícita (Alpaydin, 2010).

El aprendizaje automático se refiere al diseño y desarrollo de algoritmos y modelos que permiten a las computadoras aprender de datos y experiencias pasadas para realizar tareas específicas o tomar decisiones sin intervención humana (Bishop, 2006).

El aprendizaje automático es el proceso mediante el cual una máquina es capaz de aprender de forma automática a partir de datos, identificar patrones y tomar decisiones o hacer predicciones sin ser programada explícitamente (Murphy, 2012).

El aprendizaje automático se refiere a la capacidad de las máquinas para adquirir conocimiento y habilidades a través de la experiencia, permitiéndoles realizar tareas específicas y mejorar su rendimiento con el tiempo (Samuel, 1959).

El aprendizaje automático implica el desarrollo y uso de algoritmos y técnicas que permiten a las máquinas aprender de los datos, adaptarse a nuevas situaciones y realizar tareas sin una programación detallada (Trevor et al., 2009).

Existen diferentes enfoques dentro del aprendizaje automático, siendo los más relevantes:

a. Aprendizaje supervisado

En el aprendizaje automático supervisado, se entrena un modelo utilizando datos etiquetados, es decir, datos que contienen ejemplos de entrada y la salida deseada correspondiente. El objetivo del modelo es aprender una función que pueda mapear nuevas entradas a salidas esperadas. En otras palabras, el modelo se entrena para predecir la salida correcta o etiqueta para nuevas instancias basándose en los ejemplos de entrenamiento proporcionados. Los modelos supervisados se utilizan comúnmente para tareas de clasificación y regresión.

En ese sentido, un modelo supervisado es un algoritmo de aprendizaje automático que utiliza datos de entrenamiento etiquetados para aprender una función que puede predecir la salida correspondiente a nuevas instancias no

etiquetadas (Trevor et al., 2009). Asimismo, Alpaydin (2010) agrega que es un enfoque de aprendizaje automático en el que se entrena un algoritmo utilizando datos de entrada y salida conocidos para que pueda hacer predicciones precisas sobre datos no vistos previamente.

También es considerado como un método de aprendizaje automático en el que se proporcionan ejemplos de entrada y salida a un algoritmo para que pueda aprender a mapear nuevas entradas a salidas deseadas (Bishop, 2006). De manera que, Murphy (2012) menciona que es un algoritmo que aprende de ejemplos previamente etiquetados y utiliza esta información para realizar predicciones o clasificaciones sobre nuevos datos.

Un modelo supervisado es una técnica de aprendizaje automático en la que se entrena un algoritmo utilizando un conjunto de datos de entrenamiento que contiene pares de ejemplos de entrada y salida esperada. El objetivo es aprender una función que pueda generalizar y hacer predicciones precisas sobre nuevos datos no vistos (Mitchell, 1997).

El aprendizaje supervisado es un enfoque del aprendizaje automático en el que se utilizan datos etiquetados, es decir, datos que contienen ejemplos de entrada y la salida o etiqueta correspondiente. El objetivo principal del aprendizaje supervisado es entrenar un modelo o algoritmo para que pueda aprender a mapear nuevas instancias de entrada a las salidas deseadas. A través de la presentación de ejemplos de entrenamiento, el modelo busca aprender patrones y relaciones entre las características de entrada y las salidas conocidas, con el fin de hacer predicciones precisas sobre nuevos datos no vistos. El aprendizaje supervisado se utiliza comúnmente para tareas de clasificación, donde se busca asignar una etiqueta o categoría a una nueva instancia, o para tareas de regresión, donde se busca predecir un valor numérico continuo. Este enfoque requiere disponer de datos de entrenamiento adecuadamente etiquetados, lo que implica la participación y supervisión humana en el proceso de etiquetado de los datos.

b. Aprendizaje no supervisado

En el aprendizaje automático no supervisado, se trabajan con datos no etiquetados, es decir, datos que no tienen salidas o etiquetas predefinidas. El

objetivo principal es descubrir patrones interesantes, estructuras ocultas o grupos naturales dentro de los datos. Los modelos no supervisados buscan aprender relaciones intrínsecas en los datos y proporcionar una representación o comprensión mejorada de los mismos. Algunos ejemplos comunes de algoritmos no supervisados incluyen el clustering (agrupamiento) y la reducción de dimensionalidad.

En la literatura, el aprendizaje no supervisado es un enfoque de aprendizaje automático en el que se utilizan datos no etiquetados para descubrir patrones, estructuras ocultas o grupos naturales en los datos sin la necesidad de tener salidas predefinidas (Trevor et al., 2009).

El aprendizaje no supervisado es un método de aprendizaje automático en el que se exploran los datos sin la guía de etiquetas o salidas conocidas, con el objetivo de descubrir patrones subyacentes, relaciones o características intrínsecas de los datos (Alpaydin, 2010). Igualmente, Bishop (2006) lo define como un enfoque en el que se utiliza un algoritmo para buscar estructuras y patrones interesantes en los datos sin ninguna información adicional, como etiquetas o salidas conocidas.

Además, el aprendizaje no supervisado es un tipo de aprendizaje automático en el que se busca aprender una representación o comprensión mejorada de los datos sin utilizar información previa sobre las salidas esperadas. El objetivo es descubrir características relevantes, agrupaciones o relaciones ocultas en los datos (Murphy, 2012). También es considerado como un proceso de aprendizaje automático en el que se explora un conjunto de datos sin la presencia de etiquetas o salidas conocidas. El objetivo es encontrar patrones, tendencias o estructuras inherentes en los datos para obtener una mejor comprensión de estos (Mitchell, 1997).

El aprendizaje no supervisado es un enfoque del aprendizaje automático en el que se utilizan datos sin etiquetas o salidas conocidas para descubrir de manera automática patrones, estructuras o características inherentes en los datos. A través de algoritmos de agrupamiento, reducción de dimensionalidad u otras técnicas, el aprendizaje no supervisado busca encontrar relaciones y regularidades intrínsecas en los datos, proporcionando

una comprensión más profunda de los mismos. A diferencia del aprendizaje supervisado, no se requiere una guía externa para entrenar el modelo, lo que permite una exploración libre y descubrimiento de información valiosa en conjuntos de datos no etiquetados. El aprendizaje no supervisado es especialmente útil cuando se dispone de grandes cantidades de datos no etiquetados y se busca obtener conocimientos útiles o realizar segmentaciones basadas en la estructura subyacente de los datos.

c. Aprendizaje semisupervisado

El aprendizaje semisupervisado es un enfoque del aprendizaje automático que combina datos etiquetados y no etiquetados para entrenar un modelo. Utiliza la información limitada de los datos etiquetados y la estructura de los datos no etiquetados para mejorar la precisión del modelo en la predicción de nuevas instancias (Chapelle et al., 2006).

También es considerado como un método híbrido que aprovecha tanto datos etiquetados como no etiquetados para entrenar modelos. A través de la combinación de información parcialmente etiquetada y no etiquetada, se busca mejorar la capacidad de generalización y rendimiento del modelo en la predicción de nuevas instancias (Zhu & Goldberg, 2022).

Es una técnica que utiliza un conjunto de datos que contiene tanto ejemplos etiquetados como no etiquetados. Aprovecha la estructura y las relaciones subyacentes en los datos no etiquetados para mejorar la precisión y robustez del modelo entrenado (Berrendorf, 2022).

Por otro lado, el aprendizaje semisupervisado es un paradigma de aprendizaje automático que busca aprovechar la información adicional proporcionada por datos no etiquetados para mejorar la capacidad de generalización y rendimiento de los modelos entrenados con datos etiquetados limitados (Chapelle, 2010). Asimismo, Zhu et al. (2003) sostienen que es un enfoque que combina la capacidad de aprendizaje de los datos etiquetados con la capacidad de descubrimiento de patrones de los datos no etiquetados. Busca aprovechar la información latente en los datos no etiquetados para mejorar la calidad y eficiencia de los modelos entrenados.

El aprendizaje semisupervisado es un enfoque del aprendizaje automático que combina datos etiquetados y no etiquetados para entrenar modelos predictivos. A diferencia del aprendizaje supervisado, donde se requiere un conjunto de datos completamente etiquetados, el aprendizaje semisupervisado aprovecha la información adicional proporcionada por los datos no etiquetados para mejorar la capacidad de generalización y rendimiento del modelo.

d. Aprendizaje por refuerzo

El aprendizaje por refuerzo es un enfoque del aprendizaje automático en el que un agente interactúa con un entorno dinámico y toma acciones para maximizar una recompensa acumulativa. A través de un proceso de prueba y error, el agente aprende a tomar decisiones óptimas en función de las señales de recompensa o castigo proporcionadas por el entorno (Sutton & Barto, 2018).

Igualmente, Kaelbling et al. (1996) argumenta que es un paradigma de aprendizaje automático en el que un agente aprende a través de la interacción con un entorno mediante el ensayo y error. El agente toma acciones en el entorno y recibe recompensas o penalizaciones en función de su comportamiento, lo que le permite aprender una política de toma de decisiones óptima.

En ese sentido, el aprendizaje por refuerzo es un enfoque del aprendizaje automático en el que un agente aprende a tomar decisiones óptimas a través de la interacción con un entorno dinámico. A diferencia de otros métodos de aprendizaje, el aprendizaje por refuerzo se basa en la retroalimentación en forma de recompensas o castigos que el agente recibe del entorno en función de sus acciones.

En el contexto de esta investigación, se han explorado distintos modelos predictivos supervisados debido a su efectividad en problemas de clasificación binaria como la detección de transacciones sospechosas:

a. Regresión logística

La regresión logística es un modelo estadístico utilizado para modelar la relación entre una variable binaria dependiente y una o más variables independientes. Utiliza una función logística para estimar la probabilidad de que ocurra un evento de interés en función de las variables independientes (Hosmer et al., 2013).

Igualmente, Agresti (2018) sostiene que la regresión logística es un método de análisis estadístico utilizado para predecir la probabilidad de ocurrencia de un evento binario, como sí/no o éxito/fracaso. Se basa en el modelo logístico, que transforma una combinación lineal de variables independientes en una probabilidad a través de la función logística.

En esa misma línea, Kuha & Mills (2020) describe que es una técnica de modelado utilizada para predecir la probabilidad de un evento binario. A diferencia de la regresión lineal, que se utiliza para predecir valores continuos, la regresión logística se emplea cuando la variable dependiente es categórica y tiene dos categorías, como sí/no o 0/1.

Así también, es un método de aprendizaje automático supervisado utilizado para la clasificación de datos en dos categorías. Utiliza una función logística para modelar la relación entre las variables independientes y la probabilidad de pertenecer a una clase específica. Es ampliamente utilizado en problemas de clasificación binaria en diversos campos, como medicina, finanzas y ciencias sociales (Bishop, 2006).

La regresión logística, como indican Hastie et al. (2009), es ampliamente utilizada para problemas de clasificación binaria, incluida la detección de transacciones sospechosas. Este modelo presenta eficacia para evaluar la probabilidad de que una transacción sea fraudulenta.

Los modelos de regresión logística tienen tres objetivos principales. Primero, determinar la importancia de la relación entre cada variable independiente y la variable dependiente. Segundo, identificar posibles interacciones y confusión entre las variables independientes en relación con la variable dependiente, utilizando odds ratio para cada variable. Por último,

utilizar el modelo para clasificar a los individuos en las categorías presente o ausente de la variable dependiente (Field et al., 2012).

Entonces, el propósito de la regresión logística difiere del de la regresión lineal. Mientras que en la regresión lineal el objetivo es predecir el valor de una variable dependiente continua a partir de una o varias variables predictoras, en la regresión logística el objetivo es estimar la probabilidad de que ocurra un evento binario, es decir, cuando la variable dependiente Y sólo puede tomar dos valores posibles: éxito o fracaso.

La regresión logística modela esta probabilidad mediante la función logística o sigmoide, que transforma una combinación lineal de predictores en un valor comprendido entre 0 y 1, representando la probabilidad de que ocurra el evento.

Tal como se muestra en la Ecuación 3, la probabilidad de que el evento Y ocurra, dado el valor de las variables independientes, se expresa de la siguiente manera (González-Revaldería et al., 2007):

$$P(Y) = \frac{1}{1+e^{-(\beta_0+\beta_1 X_1+\beta_2 X_2+\cdots+\beta_n X_n)}} \qquad (3)$$

Donde:

- $P(Y = 1)$: Probabilidad de que el evento Y ocurra
- β_0: Constante o término independiente
- $\beta_1, \beta_2, \ldots, \beta_n$: Coeficientes asociados a cada variable predictora
- $X_1, X_2, \ldots, X_n$: Variables independientes
- e: Base de los logaritmos naturales

Cuando tenemos una única variable predictora X_1, la ecuación de la regresión logística en su forma más básica se representa mediante la Ecuación 4:

$$P(Y) = \frac{1}{1+e^{-(\beta_0+\beta_1 X_1)}} \qquad (4)$$

Los valores de estas ecuaciones pueden fluctuar entre 0 y 1. Un valor cercano a 0 indica que es altamente improbable que, Y haya ocurrido, mientras que un valor cercano a 1 indica que es muy probable que haya sucedido (González-Revaldería et al., 2007).

b. Máquinas de Soporte Vectorial (SVM)

Las Máquinas de Soporte Vectorial (SVM) son un conjunto de algoritmos de aprendizaje automático supervisado utilizados para la clasificación y regresión. SVM encuentra un hiperplano óptimo en un espacio de alta dimensión que maximiza el margen entre las clases, lo que permite una buena generalización y capacidad de clasificación en datos no vistos (Cortes & Vapnik, 1995).

Por otra parte, Burges (1998) indica que son modelos de aprendizaje automático que utilizan técnicas basadas en el concepto de separación óptima de clases mediante hiperplanos en un espacio de características. SVM busca encontrar el hiperplano que maximiza el margen entre las clases, lo que proporciona un buen rendimiento en problemas de clasificación y regresión.

Además, Shawe-Taylor & Cristianini (2004) expresan que son un método de aprendizaje automático que utiliza un enfoque geométrico para clasificar datos. SVM mapea los datos de entrada en un espacio de características de mayor dimensión y encuentra el hiperplano que mejor separa las clases utilizando vectores de soporte. Estos vectores de soporte son los puntos de datos más cercanos al hiperplano de separación y son fundamentales para el modelo SVM.

Las máquinas de soporte vectorial son un algoritmo de aprendizaje automático utilizado para la clasificación y regresión. SVM busca encontrar el hiperplano que mejor separa los datos en diferentes clases, maximizando el margen entre ellas. Además, SVM puede utilizar funciones de kernel para mapear los datos en espacios de características no lineales, lo que permite un mayor poder de representación y la capacidad de resolver problemas de clasificación no lineales (Trevor et al., 2009).

Para terminar, Cortes & Vapnik (1995) introdujeron las SVM, que se utilizan para problemas de clasificación y regresión. SVM es especialmente

eficaz en espacios de alta dimensión y es útil para identificar patrones complejos en los datos, lo que lo convierte en una opción valiosa para la detección de transacciones fraudulentas.

Al margen, Vapnik (1995) argumenta que la fórmula básica para la clasificación de SVM se expresa de la siguiente manera, tal como se observa en la Ecuación 5:

$$f(x) = sign(\sum_{i=0}^{n} \alpha_i y_i K(x_i, x) + b) \qquad (5)$$

Donde:

- $f(x)$: Es la función de decisión para una nueva instancia x.
- α_i: Coeficientes de Lagrange obtenidos durante el entrenamiento.
- y_i: Etiquetas de clase (+1 o -1) correspondientes a las instancias de entrenamiento.
- $K(x_i, x)$: Función kernel que mide la similitud entre el punto de entrenamiento x_i y la nueva instancia x
- b: Término de sesgo (bias).

El signo en la fórmula determina a qué clase pertenece la instancia de entrada x, es decir, si f(x) es positivo, se clasifica en una clase, y si es negativo, se clasifica en la otra clase.

La elección del kernel, como el kernel lineal, el kernel polinómico o el kernel gaussiano (RBF), depende del tipo de problema y de la distribución de los datos. Cabe destacar que esta fórmula es para la clasificación con SVM. Para la regresión con SVM, la fórmula es ligeramente diferente, ya que se utiliza una función de pérdida diferente y se busca ajustar una función de regresión en lugar de una función de decisión binaria

c. Redes Neuronales Artificiales (ANN)

Haykin (1999) ha sido pionero en el campo de las redes neuronales artificiales. Las ANN son modelos computacionales inspirados en el cerebro humano y son adecuadas para la detección de patrones en grandes conjuntos

de datos, lo que las hace ideales para la detección de fraudes en transacciones financieras.

Las Redes Neuronales Artificiales (ANN) son modelos computacionales inspirados en el funcionamiento del cerebro humano. Consisten en una colección interconectada de unidades de procesamiento llamadas neuronas artificiales, que trabajan en conjunto para realizar tareas de aprendizaje y reconocimiento de patrones. Las ANN son capaces de aprender y generalizar a partir de conjuntos de datos, lo que las hace ampliamente utilizadas en el campo del aprendizaje automático (Haykin, 2009).

En esa misma línea, Bishop (1995) expresa que son un tipo de modelo computacional que consiste en capas de unidades de procesamiento llamadas neuronas artificiales, que se conectan entre sí mediante pesos sinápticos. Estas redes son capaces de aprender a través del ajuste de los pesos sinápticos en función de los datos de entrada y las salidas deseadas. Las ANN son utilizadas para resolver problemas de clasificación, regresión, reconocimiento de patrones, entre otros.

También son considerados como modelos matemáticos inspirados en la estructura y funcionamiento del sistema nervioso. Están compuestas por nodos llamados neuronas artificiales, que están organizadas en capas y se conectan mediante conexiones ponderadas. Estas redes son capaces de aprender a partir de ejemplos y ajustar los pesos de las conexiones para realizar tareas de clasificación, regresión o reconocimiento de patrones (Rumelhart et al., 1986).

Son modelos de aprendizaje automático que imitan el funcionamiento de las redes de neuronas biológicas. Estas redes están compuestas por múltiples capas de unidades de procesamiento llamadas neuronas artificiales, que se conectan entre sí mediante conexiones ponderadas. Las ANN son capaces de aprender a partir de ejemplos y ajustar los pesos de las conexiones para mapear relaciones complejas entre los datos de entrada y las salidas esperadas. Son ampliamente utilizadas en problemas de

clasificación, reconocimiento de imágenes, procesamiento del lenguaje natural, entre otros (Goodfellow et al., 2016).

De acuerdo con Bishop (2006), la fórmula general que describe el cálculo en una neurona artificial se expresa en la Ecuación 6:

$$z = w_1 x_1 + w_2 x_2 + \cdots + w_n x_n + b \qquad (6)$$

Donde:

- z: Suma ponderada de las entradas multiplicadas por sus respectivos pesos más el sesgo.
- $w_1, w_2, \ldots, w_n$: Pesos sinápticos asignados a cada conexión entre la neurona actual y las de la capa anterior.
- $x_1, x_2, \ldots, x_n$: Entradas a la neurona actual (valores de la capa anterior).
- b Término de sesgo, que ajusta el punto de partida de la activación.

Una vez que se calcula la suma ponderada z, se aplica una función de activación a z para determinar la salida de la neurona. La elección de la función de activación depende del tipo de problema y puede incluir funciones como la función sigmoide, la función ReLU (Rectified Linear Unit) o la función softmax. Cabe destacar que esta fórmula se aplica a cada neurona en una red neuronal artificial y se repite en cada capa de la red durante el proceso de propagación hacia adelante (feedforward) para generar la salida final de la red.

d. Bosques Aleatorios (Random Forest)

Los Bosques Aleatorios (Random Forest) son un conjunto de modelos de aprendizaje automático que combinan múltiples árboles de decisión para realizar tareas de clasificación o regresión. Cada árbol individual se entrena en una submuestra aleatoria de los datos y produce una predicción. Luego, la predicción final se obtiene mediante la combinación de las predicciones de todos los árboles. Los bosques aleatorios son conocidos por su capacidad

para manejar conjuntos de datos grandes y complejos y por su resistencia al sobreajuste (Breiman, 2001).

Por otra parte, es un algoritmo de aprendizaje automático que utiliza un conjunto de árboles de decisión. Cada árbol se entrena en una muestra aleatoria de los datos, y las predicciones de los árboles individuales se combinan para obtener una predicción final. Los Bosques Aleatorios son eficaces para problemas de clasificación y regresión, ya que reducen el sobreajuste y tienen una buena capacidad de generalización (Liaw & Wiener, 2002).

Asimismo, Hastie et al. (2009) argumentan que son un método de aprendizaje automático que combina múltiples árboles de decisión para realizar predicciones. Cada árbol se entrena en una muestra aleatoria de los datos y, durante la construcción del árbol, se selecciona de manera aleatoria un subconjunto de características. La predicción final se obtiene mediante la votación o promedio de las predicciones de los árboles individuales. Los bosques aleatorios son conocidos por su capacidad para lidiar con datos ruidosos, tratar con variables de entrada irrelevantes y proporcionar una estimación de la importancia de las características.

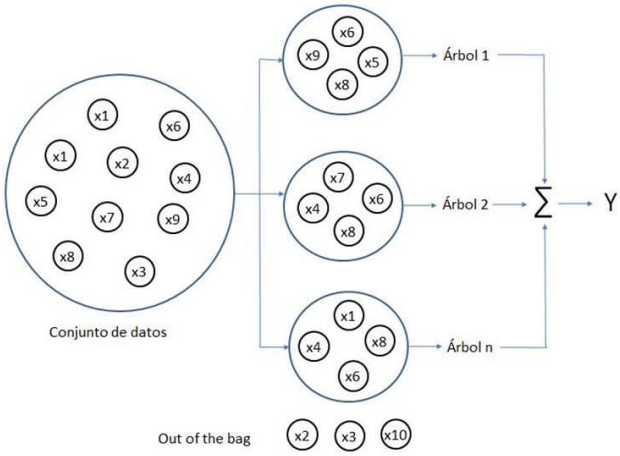
El proceso de generación de cada árbol en Random Forest consta de dos etapas. En la primera etapa, se crean numerosos árboles de decisión utilizando un subconjunto aleatorio de m variables predictivas, donde m es menor que el total de variables predictivas M. En la segunda etapa, cada árbol se desarrolla hasta alcanzar su extensión máxima (Lizares, 2017).

En la figura 4 se observa la representación gráfica del algoritmo Random Forest, Espinosa-Zúñiga (2020) menciona que cada árbol generado en Random Forest incluye un conjunto aleatorio de observaciones seleccionadas mediante la técnica de bootstrap, que permite obtener muestras de una población donde una observación puede aparecer en más de una muestra. Las observaciones no consideradas en la construcción de cada árbol (llamadas "out of the bag") se utilizan para validar el modelo. Las salidas de todos los árboles se combinan en una salida final Y, conocida como ensamblado, utilizando una regla establecida (generalmente el promedio para

salidas numéricas y el conteo de votos para salidas categóricas). Este proceso se ilustra en la Figura 4.

Figura 4

Algoritmo Random Forest



Nota. Tomado de Espinoza-Zúñiga (2020).

Random Forest es ampliamente utilizada en diversos campos debido a sus ventajas. Por ejemplo, se utiliza en teledetección para clasificar imágenes, en bancos para detectar fraudes y clasificar clientes para la concesión de créditos, en medicina para analizar historiales clínicos y detectar posibles enfermedades en los pacientes, en finanzas para pronosticar el comportamiento futuro de los mercados financieros, y en comercio electrónico para predecir si un cliente comprará o no un determinado producto, entre otros ejemplos (Cánovas et al., 2017).

e. Árbol de Decisión

El algoritmo de árbol de decisión se construye dividiendo iterativamente el conjunto de datos en subconjuntos más homogéneos, basándose en el valor de las variables predictoras. La selección del atributo que se usará para cada división no es aleatoria, sino que se realiza mediante criterios que buscan maximizar la pureza de los grupos resultantes. Uno de los criterios más utilizados en problemas de clasificación es la Ganancia de Información,

basada en la entropía, propuesta por Quinlan (1986) en su reconocido algoritmo ID3.

La entropía mide la cantidad de incertidumbre o impureza en un conjunto de datos y se calcula mediante la Ecuación 7:

$$Entropía(S) = -\sum_{i=1}^{c} p_i log_2 p_i \qquad (7)$$

Donde:

- S: Conjunto de datos en el nodo actual
- c: Número de clases en el conjunto
- p_i: Proporción de elementos pertenecientes a la clase i en el conjunto S

Un valor de entropía bajo indica un conjunto de datos más puro, es decir, que contiene elementos mayoritariamente de una sola clase. Por tanto, el objetivo del algoritmo es realizar particiones que reduzcan la entropía total del sistema.

La Ganancia de Información (IG) se emplea para cuantificar la reducción de entropía que se logra al dividir el conjunto de datos en función de un atributo específico. Esta métrica se calcula con la siguiente Ecuación 8:

$$IG(S, A) = Entropía(S) - \sum_{v \in Valores(A)} \frac{|S_v|}{|S|} Entropía(S_v) \qquad (8)$$

Donde:

- $IG(S, A)$: Ganancia de información obtenida al dividir el conjunto SSS por el atributo AAA.
- $Valores(A)$: Conjunto de valores posibles que puede tomar el atributo AAA.
- S_v: Subconjunto de S donde el atributo A toma el valor v.

El atributo que proporciona la mayor ganancia de información es seleccionado para dividir el nodo actual, ya que maximiza la reducción de la incertidumbre en la clasificación. Este proceso se repite recursivamente hasta

que se alcanzan nodos que no pueden dividirse más o que cumplen con un criterio de parada, como un número mínimo de ejemplos o una profundidad máxima del árbol.

Este método, desarrollado inicialmente en el algoritmo ID3 y luego mejorado en variantes como C4.5 y C5.0, se consolidó como una técnica esencial en el aprendizaje automático debido a su interpretabilidad, bajo costo computacional y su eficacia en problemas de clasificación (Quinlan, 1986)

f. XGBoost

El XGBoost es una implementación optimizada y escalable del algoritmo de Gradient Boosting. Es un método de aprendizaje automático que combina múltiples modelos de árboles de decisión débiles para construir un modelo de predicción más fuerte (Espinosa-Zúñiga, 2020). XGBoost utiliza un enfoque de optimización que mejora iterativamente los árboles en función de los errores residuales, lo que lo convierte en una poderosa herramienta para problemas de regresión y clasificación. La Figura 5 ilustra el funcionamiento del algoritmo XGBoost. Además, XGBoost incluye regularización y manejo eficiente de características faltantes, lo que contribuye a su rendimiento y robustez (Chen & Guestrin, 2016).

Así también, es considerado como un algoritmo de aprendizaje automático basado en Gradient Boosting que ha ganado popularidad debido a su rendimiento y eficiencia. Utiliza una combinación de árboles de decisión débiles para construir un modelo de predicción robusto y preciso (Qiu et al., 2021). XGBoost se destaca por su capacidad para manejar características faltantes, su enfoque de optimización que reduce el sobreajuste y su capacidad para manejar conjuntos de datos grandes y complejos. Debido a sus características, XGBoost ha sido ampliamente adoptado y utilizado en competiciones de ciencia de datos y aplicaciones del mundo real (Sagi & Rokach, 2021).

De acuerdo con Chen & Guestrim (2016) el algoritmo XG Boost tiene las siguientes características.

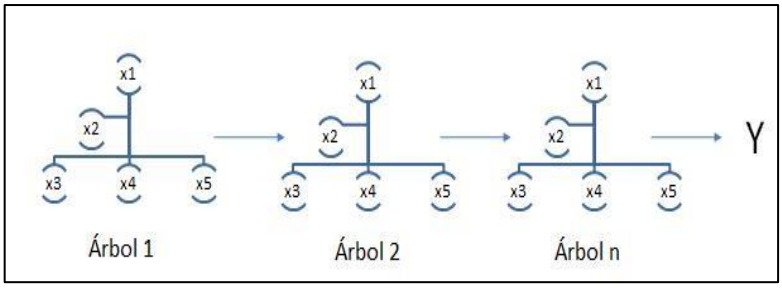
- La técnica de ensamblado secuencial de árboles de decisión, conocida como CART (Classification and Regression Trees), consiste en agregar

árboles de manera secuencial. Cada árbol se construye aprendiendo de los resultados de los árboles anteriores y corrigiendo los errores producidos por estos. Este proceso continúa hasta que no se pueda corregir más el error, utilizando un enfoque conocido como gradiente descendente.

- La principal diferencia entre los algoritmos XGBoost y Random Forest radica en que, en XGBoost, el usuario puede definir la profundidad de los árboles, mientras que en Random Forest, los árboles crecen hasta su máxima profundidad.
- El algoritmo XGBoost utiliza técnicas como el procesamiento en paralelo, la poda de árboles, el manejo de valores faltantes y la regularización (que penaliza la complejidad de los modelos) para evitar el sobreajuste o sesgo del modelo. Estas técnicas se aplican con el objetivo de lograr un mejor rendimiento y evitar problemas de ajuste excesivo.

Figura 5

Algoritmo XGBoost



Nota. Tomado de Espinoza-Zuñiga (2020).

Además, Espinoza-Zúñiga (2020) argumenta que el algoritmo XGBoost sigue el siguiente proceso:

- Inicialmente, se genera un árbol base F_0 para predecir la variable objetivo y. El residuo se calcula como la diferencia entre la predicción F_0 y el valor real de y.

- Luego, se entrena un nuevo árbol h_1 que busca predecir los residuos obtenidos en el paso anterior.
- Posteriormente, se combinan los resultados del árbol inicial y el nuevo árbol entrenado para generar un nuevo modelo, mediante la siguiente Ecuación 9:

$$F_1(x) = F_0(x) + h_1(x) \qquad (9)$$

- Este proceso se repite de manera iterativa, ajustando un nuevo árbol h_m en cada iteración, con el fin de minimizar el error residual. La función de predicción general en la iteración m se expresa como en la Ecuación 10:

$$F_m(x) = F_{m-1}(x) + h_m(x) \qquad (10)$$

De esta manera, el modelo final es una suma de árboles sucesivos que se enfocan en corregir los errores de los modelos previos.

Adicionalmente, el algoritmo XGBoost tiene varias ventajas significativas: puede manejar grandes conjuntos de datos con múltiples variables, puede manejar valores perdidos en los datos, proporciona resultados de alta precisión en las predicciones y tiene una ejecución rápida, lo que significa que es eficiente en términos de tiempo de procesamiento.

g. K-Nearest Neighbors (KNN)

El algoritmo de K-Nearest Neighbors (KNN) es un método de aprendizaje supervisado utilizado tanto en problemas de clasificación como de regresión. Su funcionamiento se basa en la premisa de que las instancias similares tienden a encontrarse en proximidad dentro del espacio de características, lo que se conoce como el principio de proximidad o vecindad (Cover & Hart, 1967)

KNN clasifica un nuevo dato analizando los K vecinos más cercanos en el conjunto de entrenamiento. La clasificación del nuevo punto se asigna

según la clase mayoritaria entre sus vecinos cercanos (en clasificación), o mediante el promedio en el caso de regresión.

Para determinar qué tan “cercano” es un punto respecto a otro, se utilizan diferentes métricas de distancia, siendo la más común la distancia Euclidiana, definida como la Ecuación 11:

$$d(x, y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \qquad (11)$$

Donde:

- $d(x, y)$: Distancia Euclidiana entre dos puntos x y y.
- x_i, y_i Valores de la característica i-ésima de los puntos x y y.
- n: Número de características o dimensiones.

Una vez calculadas las distancias entre el nuevo punto y todos los puntos del conjunto de entrenamiento, se seleccionan los K puntos más próximos y se asigna la clase predominante entre ellos. La elección del valor de K es crucial para el desempeño del algoritmo:

- Un valor de K bajo puede hacer que el modelo sea sensible al ruido y al sobreajuste.
- Un valor de K alto puede suavizar demasiado la frontera de decisión, reduciendo la precisión.

Entre sus ventajas, destaca la simplicidad y facilidad de implementación, además de que no requiere un proceso de entrenamiento explícito. Sin embargo, sus principales limitaciones son el alto costo computacional durante la predicción, especialmente con grandes volúmenes de datos, y la sensibilidad a la escala de las variables, por lo que suele ser necesario normalizar o estandarizar los datos previamente.

Estos modelos han sido ampliamente utilizados en el sector financiero para abordar el problema del lavado de activos, dada su capacidad para procesar grandes volúmenes de datos y detectar patrones anómalos que podrían pasar desapercibidos mediante métodos tradicionales.

2.2.3 Metodología basada en MLOps

La presente investigación adopta el enfoque de MLOps (Machine Learning Operations) como marco metodológico para el desarrollo y gestión de modelos predictivos orientados a la detección de transacciones sospechosas de lavado de activos. MLOps integra prácticas de DevOps, ciencia de datos y aprendizaje automático, proporcionando un enfoque sistemático y automatizado para el manejo integral del ciclo de vida de los modelos de machine learning (Ordoñez et al., 2023).

De acuerdo con Kreuzberger, Kühl & Hirschl (2022), el objetivo principal de MLOps es garantizar la confiabilidad, escalabilidad y mantenimiento continuo de los modelos, permitiendo que estos pueden ser desarrollados, desplegados y monitoreados de forma eficiente en ambientes productivos.

A continuación, se describen las etapas que comprende el enfoque MLOps, precisando que en la presente investigación solo se abarcan hasta la evaluación de modelos, excluyendo las fases de despliegue y monitoreo, las cuales forman parte del ciclo completo, pero no se consideran dentro del alcance académico de este estudio.

a. **Ingesta y comprensión de los datos:** Esta etapa comprende la identificación, recolección y exploración de los datos que serán utilizados para entrenar los modelos predictivos. Implica definir las fuentes de datos, consolidar la información y realizar un análisis exploratorio de datos (EDA) para:
    - Detectar la calidad de los datos (valores nulos, duplicados, inconsistencias).
    - Analizar la distribución de las variables.
    - Identificar correlaciones y patrones iniciales.
    - Detectar el desbalance en las clases.

    Según Sculley et al. (2015), una comprensión adecuada de los datos es crucial para evitar problemas posteriores en el desarrollo del modelo, especialmente en contextos donde los datos son dinámicos o presentan distribuciones cambiantes.

b. **Preparación y preprocesamiento de los datos:** En esta fase se realizan procesos orientados a optimizar la calidad y estructura de los datos para el entrenamiento de modelos, Entre las principales actividades se incluyen:

   - Limpieza de datos: Eliminación o imputación de valores faltantes
   - Transformación de variables categóricas: Aplicando técnicas como One Hot Encoding o Label Encoding.
   - Normalización o estandarización: Especialmente útil en algoritmos que son sensibles a la escala, como SVM o KNN.
   - Tratamiento del desbalance: Utilizando técnicas como SMOTE (Synthetic Minority Over-sampling Technique) para equilibrar el número de clases, lo cual es crítico en problemas de detección de fraude o lavado de activos (Chawla et al.,2002)

   La calidad del preprocesamiento impacta directamente en el rendimiento de los modelos predictivos y en la robustez de sus resultados.

c. **Experimentación y selección de modelos:** En esta fase se realiza la selección y experimentación con diferentes algoritmos de machine learning, evaluando su desempeño frente al problema planteado. Incluye:

   - Entrenamiento de modelos supervisados como Regresión Logística, Árbol de Decisión, Random Forest, SVM, KNN, Redes Neuronales y XGBoost.
   - Ajuste de Hiperparámetros mediante técnicas como Grid Search o Random Search, que permiten optimizar el comportamiento de cada algoritmo (Bergstra & Bengio, 2012).
   - Validación cruzada K-Fold: Para asegurar la estabilidad y generalización del modelo en diferentes subconjuntos de datos (Kohavi, 1995)

   Esta etapa es fundamental para determinar el modelo con el mejor desempeño de acuerdo con las métricas definidas.

d. **Validación y evaluación de modelos:** La evaluación se lleva a cabo mediante el cálculo de métricas de desempeño específicas para problemas de clasificación binaria:
    - Precisión (Precision): Proporción de predicciones positivas que fueron correctas.
    - Sensibilidad (Recall): Capacidad del modelo para identificar correctamente los positivos reales.
    - Área Bajo la Curva ROC (AUC-ROC): Evalúa la capacidad del modelo para distinguir entre clases a través de diferentes umbrales.

    Estas métricas permiten seleccionar el modelo que presente el mejor equilibrio entre la detección de transacciones sospechosas y la minimización de falsos positivos.

e. **Despliegue e implementación:** El despliegue de modelos consiste en integrar el modelo seleccionado dentro de un entorno productivo, permitiendo realizar predicciones en tiempo real o sobre datos actualizados periódicamente. Esta fase puede incluir la creación de APIs, microservicios o pipelines automatizados para facilitar el acceso al modelo.

    Se reconoce que, en aplicaciones empresariales, el despliegue es crítico para la adopción efectiva de modelos predictivos (Ordoñez et al., 2023)

a. **Monitoreo y mantenimientos**: La última etapa en el enfoque MLOps es el monitoreo del desempeño del modelo en producción, con el fin de detectar la pérdida de precisión o la presencia de data drift. Esto permite determinar cuándo es necesario reentrenar el modelo para adaptarlo a nuevas condiciones de los datos. Su relevancia es ampliamente reconocida en la literatura para garantizar la vigencia y efectividad de los modelos desplegados (Kreuzberger et al., 2022).

2.3 MARCO CONCEPTUAL

2.3.1 Lavado de activos

El lavado de activos es un delito que busca ocultar o disimular la naturaleza, origen, ubicación, propiedad o control de dinero y/o bienes obtenidos ilegalmente. El objetivo final del proceso es integrar el capital ilícito en la economía general y transformarlo en bienes y servicios lícitos. El lavado de activos implica introducir en la economía activos de procedencia ilícita, dándoles apariencia de legalidad al valerse de actividades lícitas, lo que permite a delincuentes y organizaciones criminales disfrazar el origen ilegal de su producto, sin poner en peligro su fuente (United Nations Office on Drugs and Crime [UNODC], 2022).

Siguiendo a Cuellar (2018), se aborda el lavado de activos como una estrategia delictiva compleja que implica la ocultación de fondos obtenidos ilegalmente para aparentar su origen legítimo.

Según el Grupo de Acción Financiera Internacional (GAFI, 2020) examina cómo el lavado de dinero puede desestabilizar economías y mercados globales, generando inflación y pérdida de ingresos fiscales. Cabe destacar que este es un organismo intergubernamental global que lidera la lucha contra el lavado de dinero, el financiamiento del terrorismo y el financiamiento de la proliferación.

Por otro lado, en base en las recomendaciones del GAFI, se estudian las regulaciones internacionales y convenios como la UNCAC para establecer pautas globales en la prevención del lavado de activos (United Nations Convention Againts Corruption [UNCAC], 2005).

De acuerdo con Foley et al. (2018) se explora el impacto de las tecnologías financieras y las criptomonedas en el lavado de dinero, comprendiendo cómo estas herramientas han facilitado nuevas formas de ocultar transacciones ilícitas.

Tomando como referencia a Bahamón-Jara et al. (2021), se analizan los aspectos psicológicos y motivacionales de las personas involucradas en

actividades de lavado de dinero, comprendiendo la toma de decisiones y el comportamiento manipulativo asociado con estas prácticas.

Basándose en los estudios de Zhang et al. (2018), se investigan estrategias de prevención y detección, incluyendo sistemas de monitoreo transaccional y técnicas de aprendizaje automático, para identificar patrones y comportamientos inusuales en las transacciones financieras y facilitar la detección temprana de actividades sospechosas.

2.3.2 Delito subyacente

Maiola (2015) sustenta que el blanqueo de capitales se refiere al procedimiento mediante el cual las ganancias adquiridas de manera ilegal son transformadas en apariencia de origen legítimo. Este proceso implica la utilización de diversas estrategias financieras y comerciales con el fin de ocultar la verdadera naturaleza y procedencia de los fondos ilícitos. El fraude implica la acción de engañar o defraudar a una persona con el propósito de obtener beneficios económicos de manera deshonesta. Este tipo de delito puede adoptar diferentes formas, como el fraude financiero, electrónico, de seguros, entre otros (Al-Hashedi & Magalingam, 2021).

En mi opinión, el blanqueo de capitales se refiere al proceso mediante el cual las ganancias ilegales son disfrazadas para que parezcan legítimas. Se utilizan diversas estrategias financieras y comerciales con el objetivo de ocultar la verdadera naturaleza y origen de los fondos ilícitos. Por otro lado, el fraude implica la acción de engañar o defraudar a alguien con el propósito de obtener beneficios económicos de manera deshonesta. Este tipo de delito puede presentarse en diferentes formas, como el fraude financiero, electrónico, de seguros, entre otros.

Por otra parte, Bravo-Acevedo (2021) argumenta que el tráfico de personas implica el reclutamiento, transporte o traslado de personas utilizando medios ilegales, con el fin de explotarlas sexualmente, laboralmente o para otros fines. Es una grave violación de los derechos humanos y una forma de esclavitud moderna (Castillo-Ramos y Muriel-Páez, 2023).

Así también, el robo es la apropiación ilegal de bienes o propiedad ajena sin consentimiento y con el uso de fuerza, violencia o intimidación (Loría & Salas, 2019). Puede incluir robos a mano armada, robos de vehículos, robos en domicilios, entre otros (Saavedra-Leyva et al., 2021).

Finalmente, Souto-Zabaleta et al. (2019) menciona que el narcotráfico es el comercio ilegal de sustancias controladas, como drogas ilegales. Implica la producción, distribución y venta de drogas con fines ilícitos. Está asociado con delitos como el contrabando de drogas, el lavado de dinero y la posesión de drogas con fines de venta (Luna-Galván et al., 2021).

2.3.3 Actividades que implican el lavado de activos

En ese marco tenemos, el fondo lícito se refiere a los recursos financieros o activos que provienen de actividades ilegales o delictivas, como el tráfico de drogas, el contrabando, el fraude, la corrupción, el lavado de dinero, entre otros (De Cunto, 2021). Estos fondos se obtienen fuera del marco legal y pueden ser utilizados para actividades ilegales adicionales o para aparentar una apariencia legítima a través del blanqueo de capitales.

Asimismo, los fondos ilegales hacen referencia a los recursos económicos o activos que se generan o adquieren en violación de las leyes y regulaciones vigentes. Estos fondos están asociados con actividades criminales, como el robo, el fraude, el contrabando, la evasión fiscal, entre otros, y su origen no cumple con los requisitos legales establecidos (Ponce-Andrade et al., 2019).

Además, los fondos provenientes de actividades ilícitas enfatizan la utilización de los recursos financieros o activos que se obtienen a través de actividades que están expresamente prohibidas por la ley, como el tráfico de drogas, la trata de personas, el terrorismo, el contrabando, la extorsión, entre otras. Estos fondos se generan de manera ilegal y están asociados con la comisión de delitos (Alvear & Micheli, 2019).

Por último, los fondos de origen delictivo son los recursos económicos o activos que tienen su origen en actividades delictivas o ilegales. Estos fondos provienen de acciones criminales como el fraude, el lavado de dinero,

el narcotráfico, el soborno, la malversación de fondos, entre otros. Su obtención no cumple con los marcos legales y éticos establecidos (Fernández-Murillo et al., 2022).

2.3.4 Inteligencia artificial

La inteligencia artificial se refiere a la capacidad de las máquinas de imitar o simular la inteligencia humana para realizar tareas de manera autónoma, como el aprendizaje, el razonamiento, la percepción y la toma de decisiones (McCarthy et al., 2006). En el campo de estudio se ocupa de crear sistemas informáticos capaces de realizar tareas que normalmente requieren inteligencia humana, como el reconocimiento de voz, la visión por computadora, la comprensión del lenguaje natural y el aprendizaje (Russell & Norvig, 2004).

Por otra parte, Winston (1992) argumenta que la tecnología permite a las máquinas realizar tareas que normalmente requieren la inteligencia humana, como el razonamiento, el aprendizaje, la percepción, la planificación y la resolución de problemas. En ese sentido, la inteligencia artificial es la disciplina que se ocupa de crear programas y sistemas capaces de exhibir comportamientos que, si fueran realizados por seres humanos, se consideran inteligentes (Ricardo et al., 2021).

La inteligencia artificial es una rama de la informática que se enfoca en la creación de sistemas y algoritmos capaces de realizar tareas que requieren inteligencia humana, como el reconocimiento de voz, el procesamiento del lenguaje natural y el aprendizaje automático (Alpaydin, 2010). Por lo tanto, se le considera como la ciencia y la ingeniería de diseñar y construir máquinas inteligentes que pueden llevar a cabo tareas con habilidad humana (Ocaña-Fernández et al., 2019).

Además, es el estudio de cómo hacer que las computadoras realicen cosas que, en el momento presente, las personas hacen mejor (Rich y Knight, 1991). En ese sentido, la inteligencia artificial es un campo de estudio que busca desarrollar sistemas y programas de computadora capaces de realizar tareas que requieren inteligencia humana, como el reconocimiento de

patrones, el procesamiento del lenguaje natural y la toma de decisiones (Norvig, 2012).

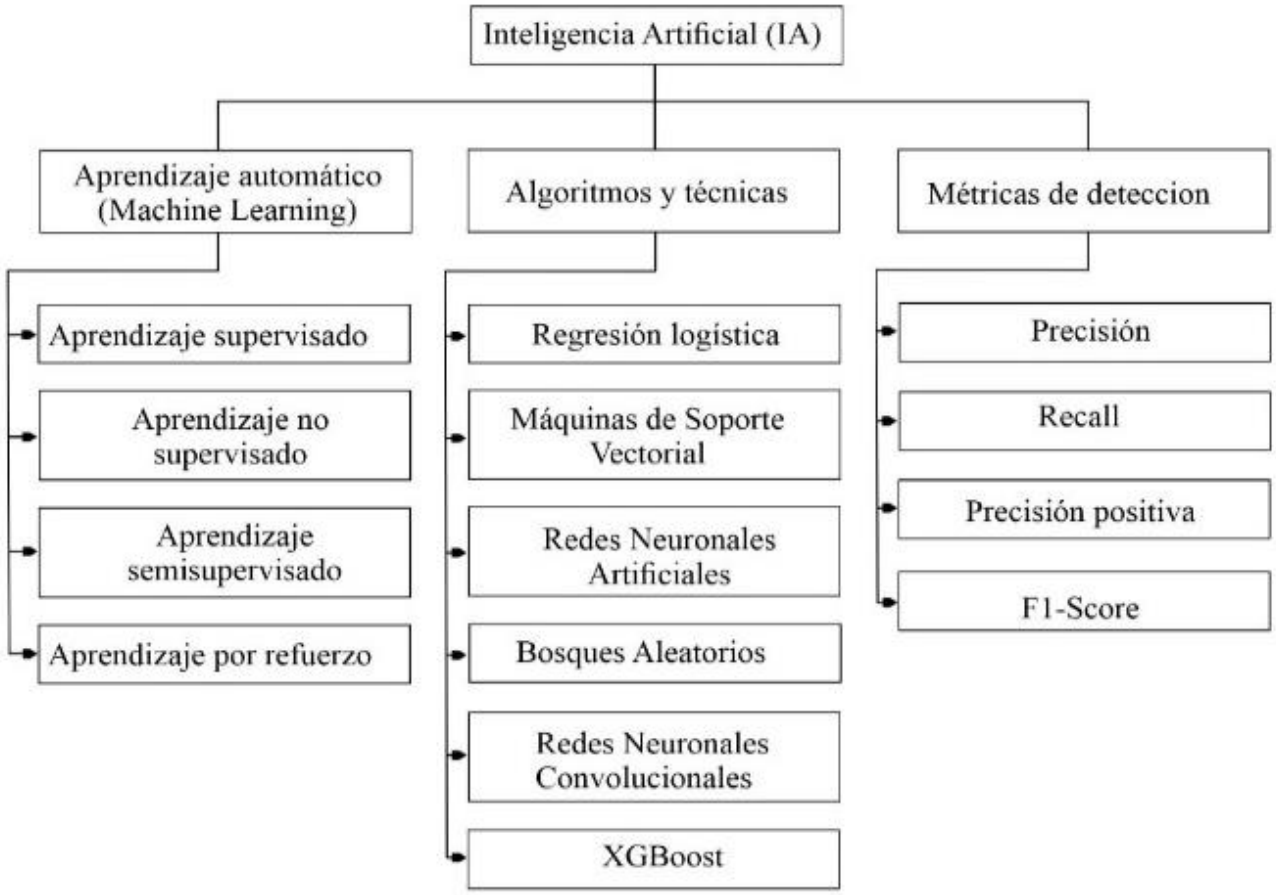
Otra definición similar sostiene que la inteligencia artificial es el conjunto de teorías y técnicas que permiten a las máquinas simular procesos cognitivos humanos, como el aprendizaje, la percepción, el razonamiento y la resolución de problemas (Pearl, 1988).

Por último, la inteligencia artificial es la rama de la informática que se ocupa del estudio y desarrollo de algoritmos y modelos que permiten a las máquinas exhibir comportamientos inteligentes y realizar tareas complejas con mínima intervención humana (Thrun et al., 2020).

En la Figura 6 se presenta un esquema conceptual de la Inteligencia Artificial (IA), en el cual se visualiza la relación entre sus principales componentes. Se destacan cuatro enfoques de aprendizaje automático: supervisado, no supervisado, semisupervisado y por refuerzo. Asimismo, se detallan los algoritmos y técnicas más utilizados. Finalmente, se incluyen las métricas clave de evaluación que permiten medir el desempeño de estos modelos. Este esquema facilita la comprensión integral de cómo la inteligencia artificial contribuye en la detección de transacciones sospechosas en el ámbito financiero.

Figura 6

Mapa conceptual de la Inteligencia artificial



Nota. Elaboración propia.

CAPÍTULO III

MÉTODO DE LA INVESTIGACIÓN

3.1 TIPO DE LA INVESTIGACIÓN

La presente investigación se clasifica como de tipo aplicada, ya que esta orientada a brindar una solución práctica a una problemática concreta en el sector financiero: la detección temprana de transacciones que podría estar relacionadas con el lavado de activos.

A diferencia de la investigación básica, que busca generar conocimientos teóricos, la investigación aplicada tiene como propósito desarrollar un modelo predictivo utilizando algoritmos como XGBoost, Random Forest, Árbol de Decisión, etc., que pueda ser implementado en entornos financieros para optimizar los procesos de detección y prevención de delitos económicos. Esto permite que los hallazgos de la investigación tengan un impacto directo en la mejora de los sistemas de vigilancia en entidades financieras.

3.2 NIVEL DE LA INVESTIGACIÓN

El nivel de la investigación es explicativo, dado que no se limita únicamente a describir las características de las transacciones financieras, sino que también busca analizar y demostrar cómo la aplicación del modelo predictivo influye en la eficacia de la detección de transacciones sospechosas.

El enfoque explicativo permite entender de qué manera los modelos como XGBoost, Random Forest, Árbol de Decisión, etc. Afecta las métricas clave del rendimiento, como la sensibilidad (recall), la precisión (precisión) y el área bajo la curva ROC (AUC-ROC), proporcionando una explicación sobre

la relación entre los patrones de las transacciones y su clasificación como sospechosas o no.

3.3 DISEÑO DE LA INVESTIGACIÓN

El diseño adoptado corresponde a un enfoque cuasi-experimental, debido a que se trabajó con un conjunto de datos simulados proporcionados por AMLSim, que recrean transacciones financieras con características tanto legítimas como de lavado de activos. En este tipo de diseño no es posible manipular las variables de forma directa en un entorno real; sin embargo, se aplican técnicas de preprocesamiento de datos, selección de variables y entrenamiento del modelo predictivo para analizar su desempeño.

Este diseño es adecuado porque permite simular la aplicación del modelo en un entorno controlado, proporcionando evidencias sobre su efectividad, lo que sienta las bases para una futura implementación en contextos reales dentro de entidades financieras

3.4 ENFOQUE DE LA INVESTIGACIÓN

El enfoque de la investigación será cuantitativo, ya que se utilizarán técnicas numéricas y estadísticas para analizar los datos recopilados. Se realizará un análisis detallado de las transacciones bancarias y se utilizarán métodos cuantitativos para medir la eficacia del modelo predictivo en la detección de operaciones sospechosas. Este enfoque proporcionará resultados numéricos y objetivos para evaluar la efectividad del modelo.

3.5 VARIABLES DE LA INVESTIGACIÓN

En la presente investigación se determinan dos variables fundamentales que estructuran el desarrollo metodológico del estudio, orientado a la creación de un modelo predictivo que permita identificar transacciones financieras potencialmente vinculadas al lavado de activos en entidades financieras.

a. **Variable Independiente (VI):**

- **Nombre:** Modelo predictivo basado de aprendizaje automático
- **Definición conceptual:** Un modelo predictivo es un tipo de modelo estadístico o computacional diseñado para estimar la probabilidad de que ocurra un evento futuro, basado en algunos datos históricos (Shmueli, 2010). En el contexto del aprendizaje automático, estos modelos se basan en algoritmos de aprendizaje supervisado que descubren patrones intrincados dentro de los datos con el propósito de hacer predicciones. Este estudio se centra en modelos utilizados para la clasificación binaria de transacciones financieras como sospechosas o no sospechosas, utilizando algoritmos ampliamente adoptados en la literatura como la regresión logística, máquinas de vectores de soporte (SVM), redes neuronales artificiales, árboles de decisión, bosques aleatorios, k-vecinos más cercanos (KNN) y XGBoost, debido a su capacidad para manejar datos de alta dimensión y su solidez en la detección de anomalías (Zhou, 2012; Géron, 2019).
- **Definición operativa:** Un modelo predictivo se implementa configurando Hiperparámetros específicos, entrenando el modelo en un conjunto de datos simulado de transacciones financieras y evaluando su rendimiento utilizando métricas de clasificación de referencia en el campo de aprendizaje automático.
- **Indicadores:**
    i. Hiperparámetros

b. Variable Dependiente (VD):

- **Nombre:** Detección de transacciones de lavado de activos
- **Definición conceptual:** La detección de transacciones de lavado de activos es una estrategia clave para prevenir delitos financieros que intentan integrar fondos obtenidos ilícitamente

en el sistema económico. En el caso del Grupo de Acción Financiera (GAFI, 2020), el lavado de dinero es ocultar o disfrazar el origen ilegal de los fondos, y constituye una amenaza directa para la integridad del sistema financiero. En este sentido, las instituciones financieras necesitan utilizar medidas proactivas que ayuden a identificar transacciones atípicas o fuera de lo común que involucren las llamadas transacciones sospechosas de lavado de activos.

- **Definición operativa:** La evaluación de esta variable se lleva a cabo con el uso de indicadores estadísticos que se obtienen después de ejecutar un modelo en un conjunto de datos de prueba utilizando métricas de sensibilidad, precisión y el área bajo la curva ROC.
- **Indicadores:**
  i. Sensibilidad (Recall): Habilidad del modelo para identificar correctamente las transacciones sospechosas (Fawcett, 2006).
  ii. Precisión (Precision): Proporción de predicciones positivas que son verdaderamente sospechosas.

Área Bajo la Curva ROC (AUC-ROC): Medida que refleja la capacidad del modelo para distinguir entre transacciones sospechosas y no sospechosas.

3.6 OPERACIONALIZACIÓN DE LAS VARIABLES

En la presente investigación, se definieron las variables que guían el estudio, así como sus respectivas dimensiones, indicadores y escalas de medición. Esta estructuración facilita la identificación y evaluación precisa de los elementos involucrados en el problema de investigación. A continuación, en la Tabla 1, se presenta la operacionalización de las variables que componen el estudio, diferenciando entre la variable independiente y la variable dependiente, junto con los criterios que permiten su medición:

Tabla 1

Operacionalización de las variables

Variables	**Dimensión**	**Indicador**	**Escala de medición**
Modelo predictivo de aprendizaje automático (VI)	Configuración del algoritmo	Hiperparámetros configurados	Nominal
Detección de transacciones de lavado de activos (VD)	Efectividad en la clasificación	Sensibilidad (Recall),	Porcentaje (%)
	Precisión en la clasificación	Precisión (Precision)	Porcentaje (%)
	Capacidad discriminativa	Área Bajo la Curva ROC (AUC-ROC)	Porcentaje (%)

Nota. Elaboración propia

3.7 POBLACIÓN Y MUESTRA

La población total analizada en este estudio está compuesta por 6,924,049 transacciones simuladas, extraídas de la base de datos AMLSim de IBM. Ante la magnitud de la población, se estima indispensable recurrir a un mecanismo de muestreo que contribuye a disminuir la carga computacional sin comprometer la representatividad de los datos, ni la validez de los resultados.

Inicialmente, se utilizó la Ecuación 12 para población finita para estimar la muestra adecuada al 95% de confianza, 0.5 de esperanza y 1% de margen de error. Bajos estos valores, el cálculo teórico para el amaño de muestra fue:

$$n = \frac{N.Z^2.p.(1-p)}{e^2.(N-1)+Z^2.p.(1-p)} \qquad (12)$$

Donde:

- N =6,924,049 (tamaño de la población)
- Z =1.96 (valor z para 95% de confianza)
- p =0.5 (proporción esperada)
- e =0.01 (margen de error)

Sustituyendo los valores, resultó un tamaño muestral de 9,592 registros.

Sin embargo, después de realizar un análisis exploratorio de cómo se distribuyen las transacciones diarias, se encontró, que una muestra ligeramente más grande de 10,568 transacciones permitió capturar los patrones temporales de la población con mayor precisión. Esta mejora se ilustra en la Figura 8, donde la frecuencia diaria de transacciones en la muestra mantiene una forma y un comportamiento que son muchos más parecidos a la población, como se muestra en la Figura 7, lo que apoya la decisión metodológica tomada.

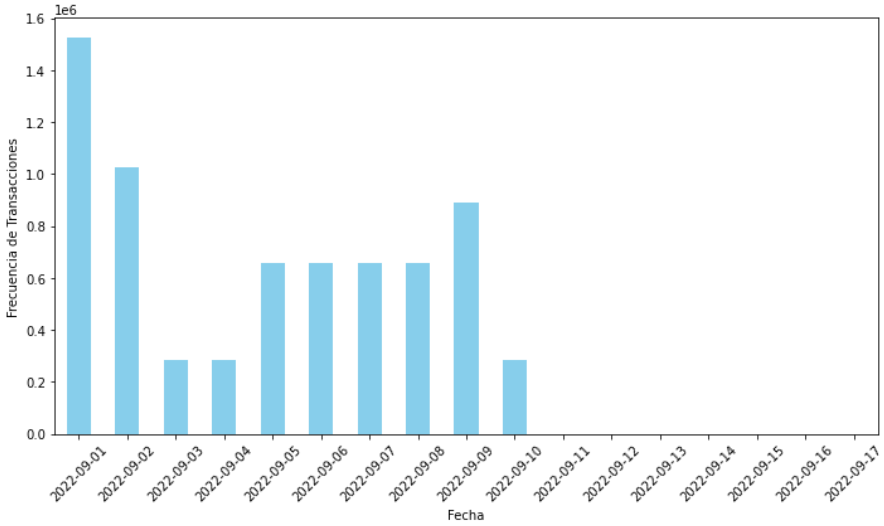
Para el caso de esta investigación, utilizamos el muestreo aleatorio sistemático, el cual consiste en seleccionar elementos de una población a intervalos regulares comenzando a partir de un punto aleatorio en la población. El intervalo de selección k se calcula con la siguiente fórmula:

$$k = \frac{N}{n} = \frac{6{,}924{,}049}{10{,}568} = 655 \qquad (13)$$

Con el intervalo de selección calculado, se elige un número inicial de manera aleatoria en el rango de 1 hasta el 655. Posteriormente, se toma cada 655. Esta metodología asegura que todos y cada uno de los elementos de la población tuvieran la misma probabilidad de ser seleccionados y, en el caso de este estudio, la aleatoriedad y representatividad se dio en el muestreo.

Figura 7

Distribución de la frecuencia de transacciones diarias en la población

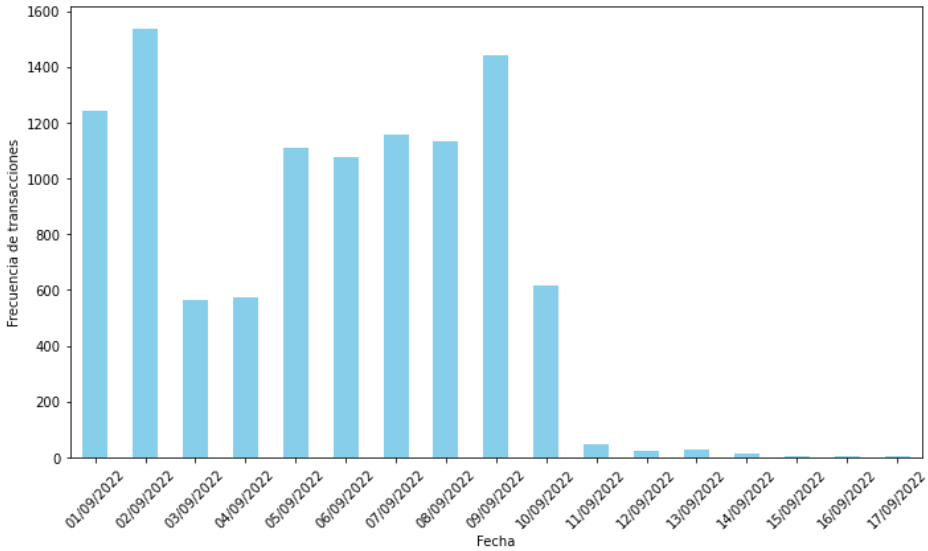


Nota. AMLSim-IBM

Elaboración propia.

Figura 8

Distribución de la frecuencia de transacciones diarias en la muestra



Nota. AMLSim-IBM

Elaboración propia.

3.8 TÉCNICA DE RECOLECCIÓN DE DATOS

- **Extracción de datos simulados desde repositorio abierto (AMLSim-GitHub):** La técnica empleada fue la recolección de datos mediante descarga de una base de datos pública, específicamente el conjunto de datos simulados proporcionado por el proyecto AMLSim, disponible en el repositorio oficial de IBM Research en la plataforma GitHub. Esta técnica consiste en acceder a un conjunto de datos ya estructurados y previamente generados, con el fin de utilizarlos como insumo en investigaciones científicas, sin necesidad de aplicar instrumentos directos de observación o experimentación sobre el campo de estudio real. Esta modalidad ha sido promovida para garantizar la privacidad de datos reales y fomentar la investigación en detección de delitos financieros a través de entornos simulados (Weber et al., 2018). Asimismo, permite cumplir con los lineamientos éticos y legales relacionados con el uso de información sensible en sistemas de aprendizaje automático (Vaidya et al., 2006).

3.9 INSTRUMENTO DE RECOLECCIÓN DE DATOS

- **Lenguaje de programación Python y sus bibliotecas especializadas como instrumento computacional de recolección y procesamiento de datos simulado:** Para trabajar con la base de datos AMLSim, se utilizó como instrumento principal el lenguaje de programación Python, debido a su flexibilidad, potencia y amplia adopción en el ámbito del análisis de datos y aprendizaje automático. Python ha demostrado ser una herramienta clave en entornos de detección de fraudes financieros gracias a su ecosistema de bibliotecas como Pandas, Numpy y Scikit-learn (Pedregosa et al., 2011).

3.10 MÉTODO DE ANÁLISIS DE DATOS

El análisis de datos en la presente investigación se efectuó mediante técnicas de minería de datos y aprendizaje automático, orientadas a

desarrollar modelos predictivos que permitan la identificación oportuna de transacciones sospechosas de lavado de activos en el sector financiero.

Inicialmente, se realizó un análisis exploratorio de datos (EDA) para comprender la distribución y comportamiento de las variables obtenidas a partir del simulador AMLSim (Suzumura & Kanezashi, 2021), permitiendo identificar patrones y características relevantes en las transacciones. A continuación, se procedió al preprocesamiento de datos, que incluyo la transformación de variables, balanceo de clases y la selección de características significativas para la predicción (Han, Kamber & Pei, 2012).

Posteriormente, se implementaron y compararon siete modelos de clasificación supervisada, ampliamente utilizados en la literatura para la detección de fraudes y anomalías:

- XGBoost (Chen & Guestrin, 2016)
- Random Forest (Breiman, 2001)
- Árbol de Decisión (Quinlan, 1986)
- Support Vector Machine (SVM) (Cortes & Vapnik, 1995)
- Redes Neuronales Artificiales (LeCun, Bengio & Hinton, 2015)
- K-Nearest Neighbors (KNN) (Cover & Hart, 1967)
- Regresión Logística (Hosmer, Lemeshow & Sturdivant, 2013)

El rendimiento de cada modelo se evaluó utilizando un conjunto de prueba independiente y considerando métricas estándar de clasificación binaria:

- Precisión (Precision)
- Sensibilidad o Recall
- F1-Score
- Área Bajo la Curva ROC (AUC-ROC) (Fawcett, 2006)

Estas métricas permitieron comparar de manera objetiva la capacidad predictiva y la robustez de cada modelo, identificando a que ofrecía el mejor desempeño en la clasificación de transacciones sospechosas.

CAPÍTULO IV

DESARROLLO DEL TRABAJO DE INVESTIGACIÓN

4.1 METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

En este apartado se presenta la aplicación práctica de la metodología MLOps definida previamente, orientada al desarrollo de modelos predictivos para la detección temprana de transacciones sospechosas de lavado de activos. La metodología consta de seis fases, de las cuales se desarrollan las cuatro primeras en esta tesis. Las dos últimas fases, la fase 5: Despliegue e implementación y fase 6: Monitoreo y mantenimiento, no se incluyen en el alcance del presente trabajo, ya que el modelo no será desplegado en un entorno productivo ni se realizará un seguimiento posterior de su rendimiento.

- Fase 1: Ingesta y comprensión de los datos
- Fase 2: Preparación y preprocesamiento de los datos
- Fase 3: Experimentación y selección de modelos
- Fase 4: Validación y evaluación de modelos
- Fase 5: Despliegue e implementación
- Fase 6: Monitoreo y mantenimiento

4.2 FASE 1: INGESTA Y COMPRENSIÓN DE LOS DATOS

La primera fase consistió en el análisis exploratorio del conjunto de datos proporcionado por el simulador AMLSim de IBM. El dataset consta de 10,568 registros distribuidos en variables categóricas y numéricas, diseñadas para simular transacciones financieras reales.

- **Conjunto de variables originales y variables derivadas**

La Tabla 2 presenta las variables del dataset AMLSim utilizadas en la investigación para el desarrollo del modelo predictivo de detección de lavado de activos. Cada variable ha sido definida con su respectiva dimensión, indicador y escala de medición, lo que permite estructurar adecuadamente la información que será procesada por los algoritmos de aprendizaje automático.

La variable dependiente IS_LAUNDERING actúa como el target del modelo, determinando si una transacción es sospechosa o no de lavado de activos, con una escala de medición cualitativa binaria. Las demás variables corresponden a características propias de cada transacción, tales como la identificación de las cuentas de origen y destino (FROM_BANK, TO_BANK, ACCOUNT, ACCOUNT.1), el tipo de moneda recibida y girada (RECEIVING_CURRENCY, PAYMENT_CURRENCY), así como el formato de pago (PAYMENT_FORMAT) y los montos involucrados (AMOUNT_RECEIVED, AMOUNT_PAID). Además, se incluye la variable TIMESTAMP, que registra la fecha y hora en que se ejecuta cada transacción, indispensable para identificar patrones temporales asociados a comportamientos anómalos.

Tabla 2

Variables del dataset AMLSim

Variables	**Dimensión**	**Indicador**	**Escala de medición**
IS_LAUNDERING (target)	Transaccional	Si / No, la cuenta está asociada a transacciones sospechosas.	Cualitativa (binaria)
FROM_BANK	Identificación	Banco dónde se origina la transacción.	Cualitativa (nominal)
ACCOUNT	Identificación	Cuenta dónde se emite	Cualitativa (nominal)

		la transacción.	
TO_BANK	Identificación	Banco destino de la transacción.	Cualitativa (nominal)
ACCOUNT.1	Identificación	Cuenta destino de cada transacción.	Cualitativa (nominal)
RECEIVING_CURRENCY	Descripción	Tipo de moneda en la que se recibe el monto de la transacción.	Cualitativa (nominal)
PAYMENT_CURRENCY	Descripción	Tipo de moneda en la que se paga o gira el monto de la transacción.	Cualitativa (nominal)
PAYMENT_FORMAT	Descripción	Tipo o formato de pago de la transacción.	Cualitativa (nominal)
AMOUNT_RECEIVED	Financiera	Monto de la transacción recibida.	Cuantitativa (continua)
AMOUNT_PAID	Financiera	Monto de la transacción pagada o girada.	Cuantitativa (continua)
TIMESTAMP	Financiera	Fecha (DD/MM/YY) y hora de la transacción.	Cualitativa (temporal)

Nota. AMLSim-IBM (https://github.com/IBM/AMLSim)

En la tabla 3 se observa que a partir de las variables originales del conjunto de datos AMLSim, se crearon 28 variables derivadas que permiten enriquecer el análisis exploratorio y fortalecer la fase de modelado predictivo.

Estas variables comprenden categorizaciones por día de la semana, franjas horarias, entidades bancarias, tipo de moneda, tipo de cambio y modalidad de transacción. La construcción de este dataset extendido facilita la identificación de patrones asociados a actividades sospechosas y mejora la capacidad explicativa de los modelos predictivos.

Tabla 3

Variables Derivadas

Variables	**Dimensión**	**Indicador**	**Escala de medición**
Entidad Bancaria (mismo banco)	Identificación	Tipo de entidad bancaria (mismo banco)	Cualitativa (binaria)
Entidad bancaria (otro banco)	Identificación	Tipo de entidad bancaria (otro banco)	Cualitativa (binaria)
Cuenta bancaria (misma cuenta)	Identificación	Cuenta bancaria (misma cuenta)	Cualitativa (binaria)
Cuenta bancaria (otra cuenta)	Identificación	Cuenta bancaria (otra cuenta)	Cualitativa (binaria)
Tipo de transacción (financiera)	Transaccional	Transacción financiera	Cualitativa (binaria)
Tipo de transacción (transferencia)	Transaccional	Transacción por transferencia	Cualitativa (binaria)
Tipo de transacción (efectivo)	Transaccional	Transacción en efectivo	Cualitativa (binaria)
Tipo de transacción (tarjeta de crédito)	Transaccional	Transacción con tarjeta de crédito	Cualitativa (binaria)
Tipo de transacción (cheque)	Transaccional	Transacción con cheque	Cualitativa (binaria)
Monto girado	Financiera	Monto girado	Cuantitativa (continua)
Monto recibido	Financiera	Monto recibido	Cuantitativa (continua)

Tipo de moneda recibido (Euro)	Descriptiva	Uso de Euro en monto recibido	Cualitativa (binaria)
Tipo de moneda girado (Euro)	Descriptiva	Uso de Euro en monto girado	Cualitativa (binaria)
Tipo de moneda recibido (Dólar)	Descriptiva	Uso de Dólar en monto recibido	Cualitativa (binaria)
Tipo de moneda girado (Dólar)	Descriptiva	Uso de dólar en monto girado	Cualitativa (binaria)
Tipo de cambio (No)	Descriptiva	No hubo tipo de cambio	Cualitativa (binaria)
Tipo de cambio (Si)	Descriptiva	Hubo tipo de cambio	Cualitativa (binaria)
Rango del día mañana	Temporal	Franja horaria: mañana	Cualitativa (binaria)
Rango del día tarde	Temporal	Franja horaria: tarde	Cualitativa (binaria)
Rango del día noche	Temporal	Franja horaria: noche	Cualitativa (binaria)
Rango del día madrugada	Temporal	Franja horaria: madrugada	Cualitativa (binaria)
Dia Lunes	Temporal	Transacción realizada el lunes	Cualitativa (binaria)
Dia Martes	Temporal	Transacción realizada el martes	Cualitativa (binaria)
Dia Miércoles	Temporal	Transacción realizada el miércoles	Cualitativa (binaria)
Dia Jueves	Temporal	Transacción realizada el jueves	Cualitativa (binaria)
Dia Viernes	Temporal	Transacción realizada el viernes	Cualitativa (binaria)
Dia Sábado	Temporal	Transacción realizada el sábado	Cualitativa (binaria)

Dia Domingo	Temporal	Transacción realizada el domingo	Cualitativa (binaria)

Nota: AMLSim-IBM

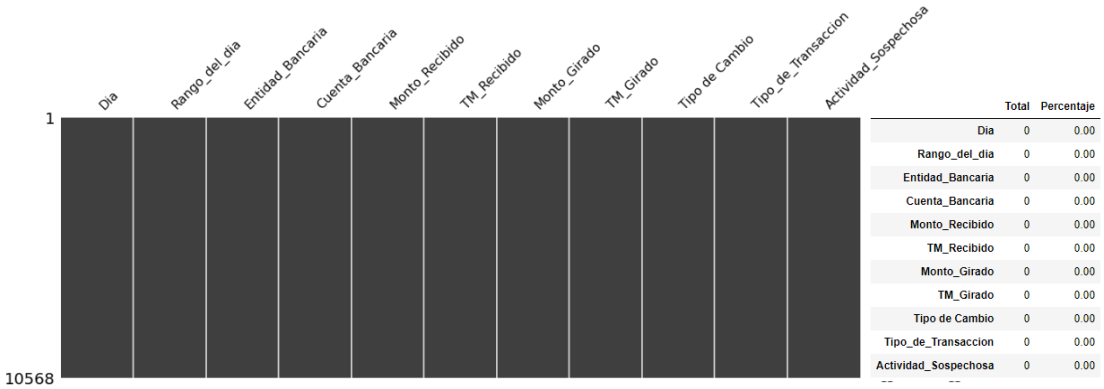
Elaboración propia

- **Validación de Nulos**

Antes de proceder con el análisis descriptivo y predictivo, se realizó el preprocesamiento de los datos con el lenguaje de programación en Python, la verificación de los valores nulos en el conjunto de datos para garantizar la calidad y la adecuación de estos para los análisis estadísticos.

Figura 9

Distribución de valores nulos por variable en el conjunto de datos



Nota. AMLSim-IBM

Elaboración propia.

En la Figura 9, se aprecia la ausencia de valores nulos por cada variable visualizando en total de frecuencias y porcentaje de valores nulos del (0%), eliminando la necesidad de imputaciones o eliminaciones de datos que podrían sesgar los resultados. Este primer análisis indica que no existen valores nulos en ninguna de las variables evaluadas: 'Día', 'Rango del día', 'Entidad Bancaria', 'Cuenta Bancaria', 'Monto Recibido', 'TM Recibido', 'Monto Girado', 'TM Girado', 'Tipo de Cambio', 'Tipo de Transacción', y 'Actividad Sospechosa'.

Hay que destacar que el conjunto de datos contempla 9 variables cualitativas o categóricas y 2 variables cuantitativas o numéricas. Por lo que, más adelante en el análisis descriptivo para las variables numéricas 'Monto Recibido' y 'Monto Girado', se optó por normalizar estos datos a través de una transformación logarítmica, ya que se utiliza para manejar datos que tienen una distribución sesgada, y es especialmente útil cuando los datos presentan una variabilidad alta o cuando los valores están distribuidos de manera no uniforme con una larga cola hacia la derecha (distribución sesgada positivamente). Ver Figura 14.

- **Análisis descriptivo**

Variables Cualitativas

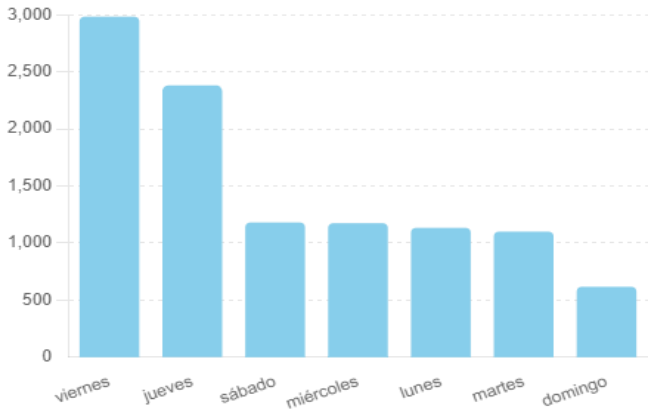
Este análisis preliminar es crucial para entender la estructura básica de los datos y detectar posibles patrones, anomalías o tendencias que podrían influir en los resultados del estudio. Además, se utilizarán representaciones gráficas para ilustrar de manera clara y concisa los hallazgos más relevantes de las variables estudiadas.

- **Análisis Univariado**

De la figura 10, se puede apreciar que el día con mayor cantidad de transacciones es el viernes, acumulando un total de 2983 transacciones de la muestra analizada, esto sugiere que el final de la semana laboral es un periodo en el cual se realizan más actividades financieras. Mientras que el día con menor cantidad de transacciones es el domingo (617), dónde baja la actividad en este día, que puede deberse a que muchas instituciones financieras y empresas reducen sus operaciones durante el fin de semana.

Figura 10

Frecuencia de transacciones por día



Nota. AMLSim-IBM

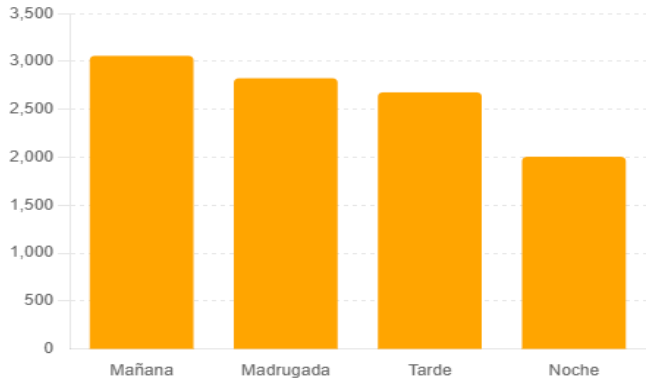
Elaboración propia.

De la figura 11, se puede apreciar que la “Mañana” es el rango horario con mayor cantidad de transacciones, acumulando un total de 3059 transacciones, sugiriendo que las primeras 6 horas del día laboral son el periodo más activo para las operaciones financieras. Asimismo, la “Tarde” presenta un volumen considerable de transacciones, dónde la actividad financiera se mantiene relativamente alta durante este periodo del día, ya que es una extensión de la jornada laboral. Mientras que la “Noche” es el rango horario con menor cantidad de transacciones, que puede ser debido que al finalizar el día la mayoría de las personas y empresas disminuyen significativamente sus actividades financieras por las horas de descanso y cese de actividades laborales o comerciales, así como el cierre en la atención de los bancos, cajas y tiendas. Por otro lado, hay que destacar que el rango de la “Madrugada” se encuentra en segundo lugar en cuanto a cantidad de transacciones, con 2825 transacciones, por lo que este periodo presenta una particularidad de actividad significativa, aunque ligeramente menor en comparación con las horas laborales estándar de la “Mañana”, lo cual se

deberá monitorear para ver porque se están dando estas operaciones durante estas horas.

Figura 11

Frecuencia de transacciones por rango de día



Nota. AMLSim-IBM

Elaboración propia.

La figura 12, muestra la frecuencia de transacciones dividida en dos categorías: "Mismo Banco" y "Otro Banco", dónde ésta última es la que presenta mayor cantidad de transacciones, con un total de 10388 transacciones, indicando que más del 98% de las transacciones financieras de la muestra analizada se realizan entre diferentes entidades bancarias. Mientras que las transacciones internas dentro de la misma entidad bancaria son menos comunes.

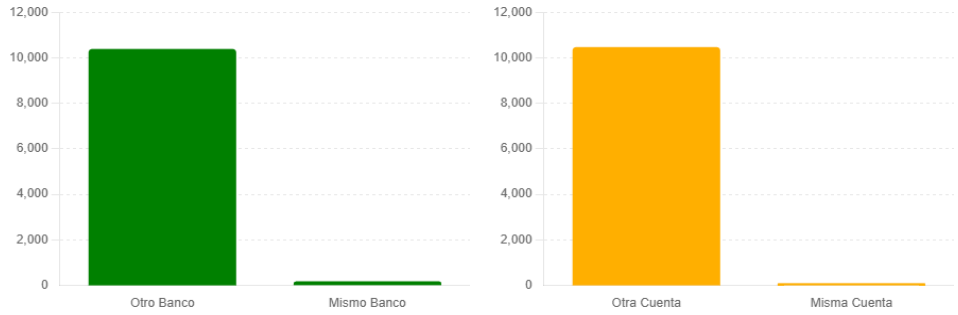
La gran diferencia entre las categorías mostradas sugiere que los clientes y las empresas prefieren realizar transacciones con otras entidades bancarias en lugar de mantener sus operaciones dentro de la misma entidad, dónde este patrón podría estar influenciado por factores como la diversificación de servicios, las tasas de cambio, y las políticas de comisiones entre bancos.

Por otro lado, tenemos, de similar manera para la categoría “Otra Cuenta” que es la que presenta la mayor cantidad de transacciones, sugiriendo que la mayoría de las transacciones se realizan entre diferentes

cuentas bancarias. Mientras que la categoría “Misma Cuenta” tiene una menor cantidad de transacciones sugiriendo que las transacciones internas dentro de la misma cuenta bancaria son bastante infrecuentes por lo que este patrón de comportamiento podría estar influenciado por la necesidad de gestionar diferentes fondos, realizar pagos a terceros, o manejar distintas actividades comerciales.

Figura 12

Frecuencia de transacciones por entidad y cuenta bancarias



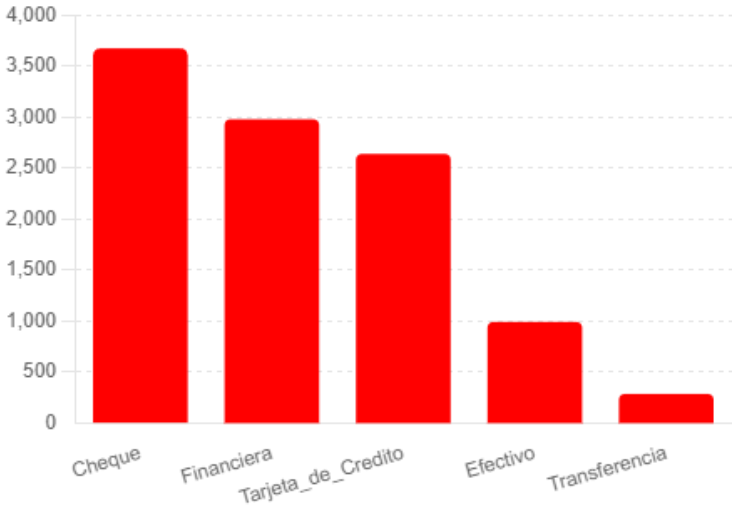
Nota. AMLSim-IBM

Elaboración propia.

En la figura 13, se muestra que el tipo de transacciones más popular entre los usuarios y empresas es el “Cheque” ya que se presenta la mayor cantidad de transacciones realizadas para la muestra analizada, con un total de 3673 registros. Le siguen las transacciones “Financieras” y transacciones por “Tarjeta de Crédito” que son también métodos cada vez más frecuentes y que son generalmente considerados más seguros y convenientes para hacer movimientos de grandes sumas de dinero o transacciones comerciales, por lo que actividades o movimientos sospechosos serían casi indetectables. Mientras que el “Efectivo” y las “Transferencias” tienen la menor cantidad de registros de transacciones, sugiriendo que estos movimientos son menos frecuentes en comparación con los otros métodos.

Figura 13

Frecuencia por tipo o método de transacciones



Nota. AMLSim-IBM

Elaboración propia.

En la figura 14, se aprecia que la “Moneda Recibida” más frecuente es el “Dólar estadounidense”, con un total de 6356 transacciones. Esto indica que la mayoría de las transacciones se realizan utilizando esta moneda, probablemente debido a su aceptación global y estabilidad. Mientras que la moneda recibida menos frecuente es el “Euro”, con un total de 4212 transacciones.

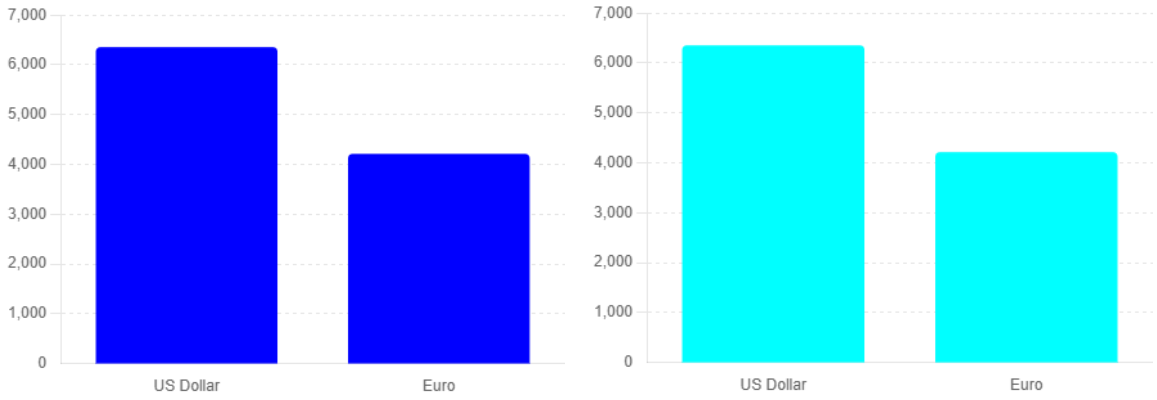
Además, la “Moneda Girada” más frecuente es también el “Dólar estadounidense”, con un total de 6354 transacciones. Esto refleja una tendencia similar a la observada en la moneda recibida, con el dólar siendo la moneda preferida para girar fondos. Mientras que la menos frecuente es el “Euro”, con un total de 4214 transacciones.

Hay que destacar que, aunque el “Euro” es menos frecuente que el “Dólar”, sigue siendo una moneda significativa en el contexto de las transacciones financieras para la casuística de estudio. Además, la alta frecuencia de transacciones en dólares estadounidenses para girar fondos sugiere que esta moneda es predominante tanto para recibir como para enviar

dinero, probablemente debido a sus ventajas en términos de estabilidad y aceptación internacional.

Figura 14

Frecuencia de transacciones por tipo de moneda recibida y girada



Nota. AMLSim-IBM

Elaboración propia.

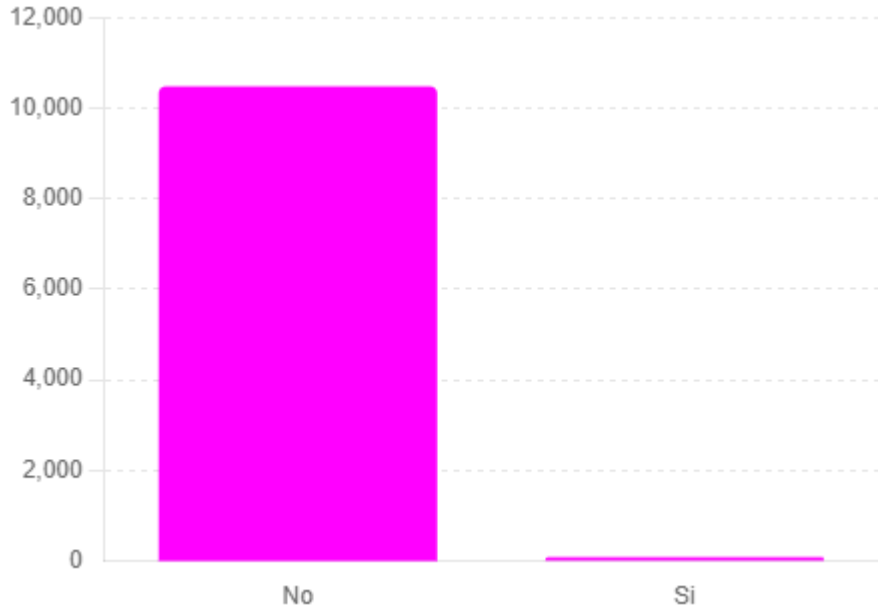
En la figura 15, muestra la frecuencia de las transacciones dividida en dos categorías: con tipo de cambio ("Sí") y sin de tipo de cambio ("No"). Dónde esta última (sin tipo de cambio) es la más frecuente, con un total de 10478 registros, indicando que la gran mayoría de las transacciones se realizan sin necesidad de convertir entre las diferentes monedas evaluadas. Mientras que en su contraparte (con tipo de cambio) tiene una menor cantidad de transacciones, con un total de 90 registros. Esto sugiere que solo una pequeña proporción menos del 1% de las transacciones registradas implican una conversión de moneda a otra.

La predominancia de transacciones sin tipo de cambio refleja una tendencia hacia la simplicidad y eficiencia en las operaciones financieras, evitando las complicaciones y posibles costos asociados cuando se realiza un giro, además en este contexto puede estar influenciado por factores externos como la estabilidad de la moneda utilizada durante el periodo de análisis, las

políticas gubernamentales, y la naturaleza de las transacciones en el sistema financiero (por ejemplo, operaciones locales versus internacionales).

Figura 15

Frecuencia de transacciones por tipo de cambio



Nota. AMLSim-IBM

Elaboración propia.

Variables Cuantitativas

De la figura 17 y figura 18, el histograma y el diagrama de cajas del "Monto Girado" y "Monto Recibido" se visualiza una distribución altamente sesgada con una mayoría de transacciones concentradas en valores relativamente bajos, como lo indica los estadísticos descriptivos de la figura 16, por lo que los valores máximos son extremadamente altos, que sugieren la presencia de valores atípicos que alteran muy significativamente las medidas de tendencia central como la media, mediana, además que hay presencia de una alta variabilidad medida a través de la desviación estándar por lo que se pueden percibir y representar que en ambos casos estas transacciones son inusuales o potencialmente sospechosas, que destacan del comportamiento típico observado de la mayoría de las transacciones.

Dado el notable sesgo y la presencia de valores extremos en las variables 'Monto Recibido' y 'Monto Girado', se recomienda aplicar una transformación logarítmica para mejorar la interpretación y análisis en el conjunto de datos, ya que una transformación ayudará a reducir la variabilidad y la escala de los valores, además de normalizar la distribución de las variables, haciéndolas más simétricas. Esta transformación logarítmica se aplicará en la fase 2 “Preparación y preprocesamientos de los datos”.

Figura 16

Estadísticos descriptivos de las variables monto recibido y girado

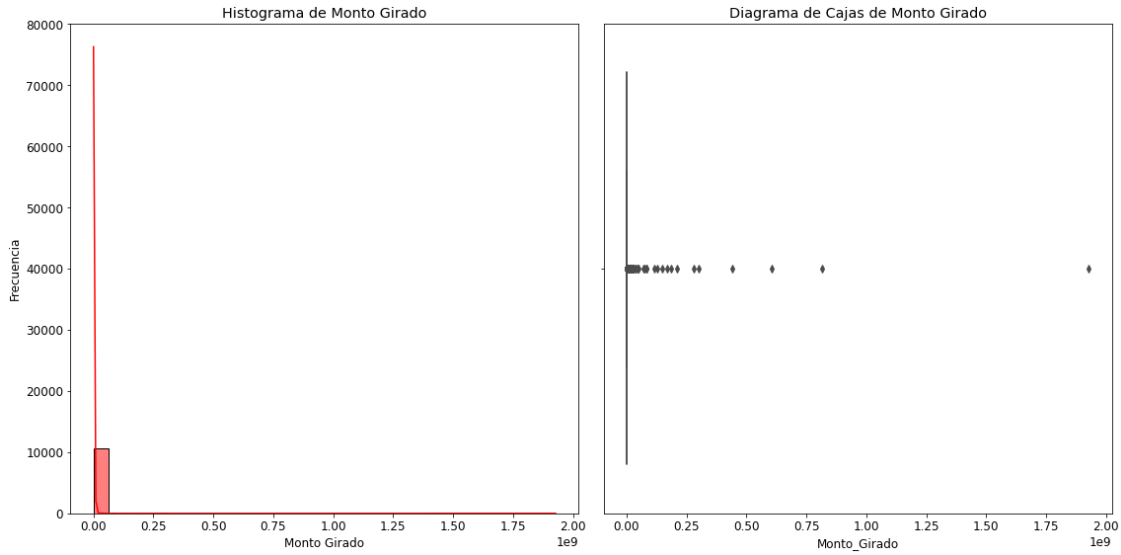
	Monto_Recibido	Monto_Girado
count	10568.00	10568.00
mean	674688.43	674638.91
std	22445879.64	22445875.82
min	0.01	0.01
25%	226.26	226.47
50%	1312.05	1312.59
75%	5482.59	5482.59
max	1927897655.00	1927897655.00

Nota. AMLSim-IBM

Elaboración propia.

Figura 17

Histograma y diagrama de cajas de la variable monto girado

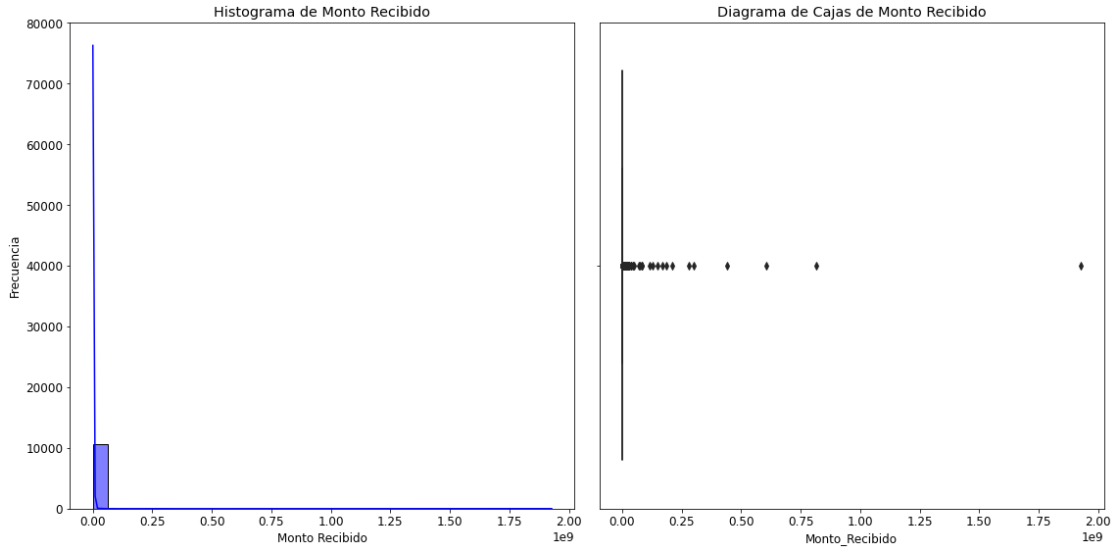


Nota. AMLSim-IBM

Elaboración propia.

Figura 18

Histograma y diagrama de cajas de la variable monto recibido



Nota. AMLSim-IBM

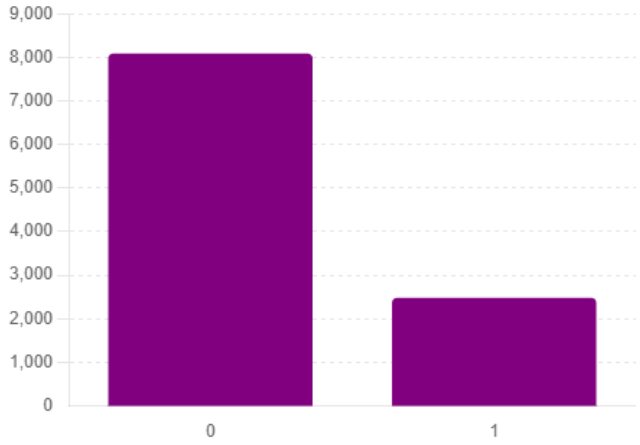
Elaboración propia.

En este apartado la figura 19, analiza la distribución de las transacciones según la categorización de la variable objetivo del estudio (“target”) que es la actividad sospechosa. Por lo que se muestra la frecuencia de las transacciones dividida en dos categorías: "No Sospechosa" (0) y "Sospechosa" (1).

La categoría “No Sospechosa” es la más frecuente, con un total de 8087 registros, indicando que el 77% de las transacciones no presentan características que las clasifiquen como sospechosas según los criterios establecidos. Se puede sugerir que la predominancia de transacciones no sospechosas refleja un sistema financiero relativamente estable y seguro, donde la mayoría de las actividades cumplen con las normativas y que posiblemente no presenten señales de riesgo. Mientras que la categoría “Sospechosa” tiene una menor cantidad de registros, con un total de 2445 transacciones, indicando una proporción del 23% que resulta ser significativa, aunque menor, pero que términos de volumen monetario podrían clasificarse como alarmantes y si fuera importante que las entidades financieras lo monitoricen.

Figura 19

Frecuencia de transacciones por actividades sospechosas



Nota. AMLSim-IBM

Elaboración propia.

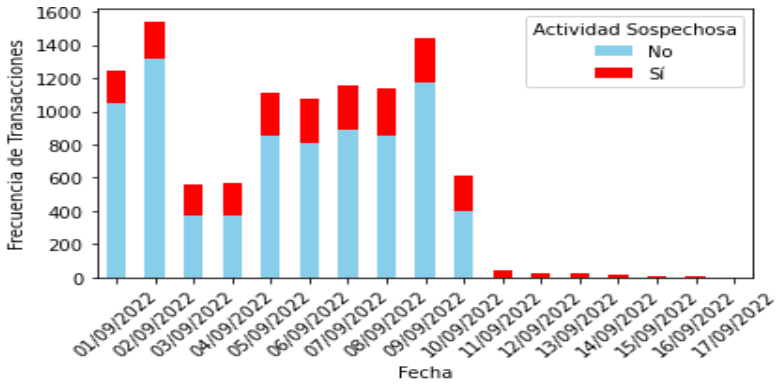
- **Análisis Bivariado**

El análisis bivariado presentado muestra las relaciones entre pares de variables o características de las transacciones bancarias para identificar patrones que sugieran una actividad sospechosa. Al examinar estas combinaciones como el día de semana, el rango de horas del día, tipo de transacción, entidad bancaria, cuenta bancaria, tipo de moneda de girada y recibida así el cómo el tipo de cambio, después de este análisis gráfico bivariado se destaca las correlaciones significativas que pueden indicar los comportamientos de actividades sospechosas o ilícitas, tales como el lavado de dinero.

En la figura 20 se muestra el análisis de la frecuencia de transacciones por día de la semana, se ha observado que la distribución de transacciones, tanto sospechosas como no sospechosas, varía significativamente a lo largo de los primeros diez días del mes actual. Este patrón continuo sugiere que estas fechas pueden estar asociadas con un volumen incrementado de incidencias sospechosas, que oscilan entre el 14,2% y el 35,0% por cada fecha, con un promedio del 24,8% para las actividades consideradas sospechosas, este comportamiento puede indicar la existencia de patrones específicos relacionados con las actividades ilícitas al inicio de un mes.

Figura 20

Frecuencia de transacciones por día y actividades sospechosas



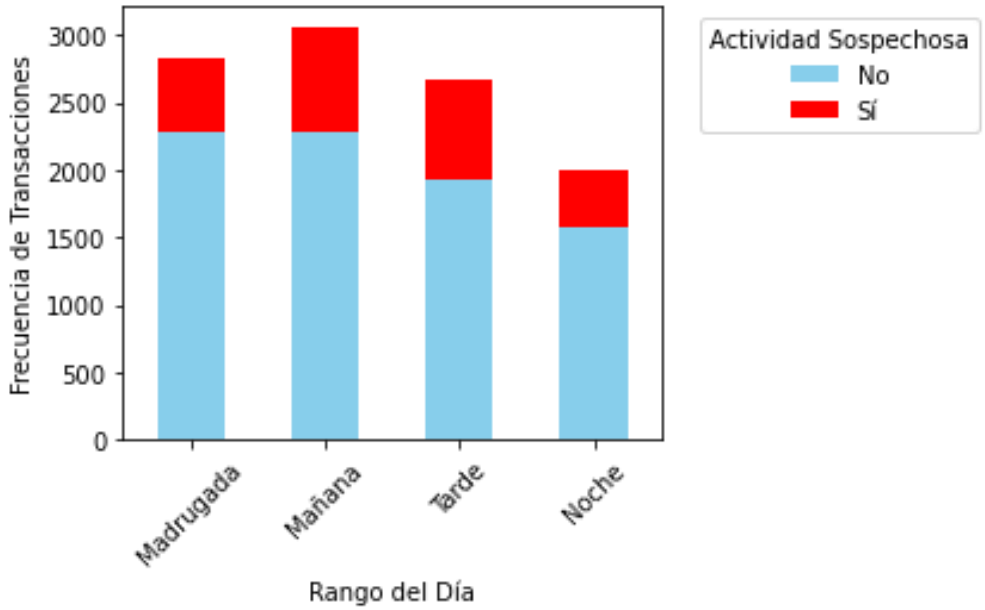
Nota. AMLSim-IBM

Elaboración propia.

En la figura 21 muestra la distribución de transacciones bancarias a lo largo de diferentes rangos de horas del día muestra que las transacciones sospechosas se concentran principalmente en horas específicas, con una proporción más alta en la mañana (25,4%) y en la tarde (27,5%), en comparación con otros periodos del día como la noche (21,2%) y la madrugada (18,9%).

Figura 21

Frecuencia de transacciones por rango de horas del día y actividades sospechosas



Nota. AMLSim-IBM

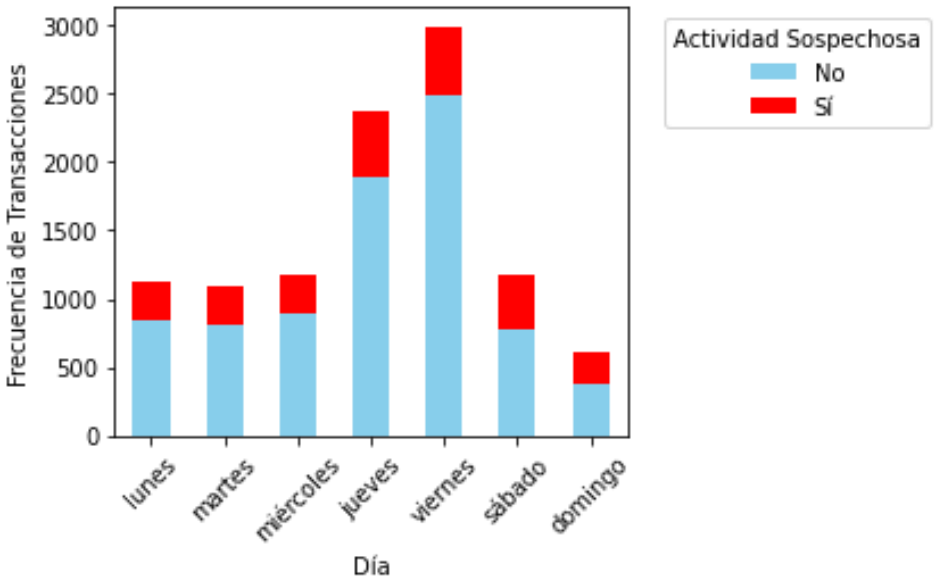
Elaboración propia.

Ahora, en la figura 22 se muestra el análisis de la distribución de transacciones bancarias, tanto sospechosas como no sospechosas, a lo largo de los días de la semana, observamos que las actividades sospechosas alcanzan su máxima frecuencia los jueves y viernes, con un pico particularmente notable el viernes, dónde esto podría sugerir que los actores ilícitos prefieren operar hacia el final de la semana laboral, posiblemente para aprovechar el menor escrutinio durante el fin de semana. A pesar de esto, los

días con las proporciones relativas más altas de actividades sospechosas son el sábado (34,9%) y domingo (39,1%), indicando que, aunque el volumen de transacciones pueda ser menor, la proporción de actividades ilícitas es considerablemente más alta durante el fin de semana.

Figura 22

Frecuencia de transacciones por días de la semana y actividades sospechosas



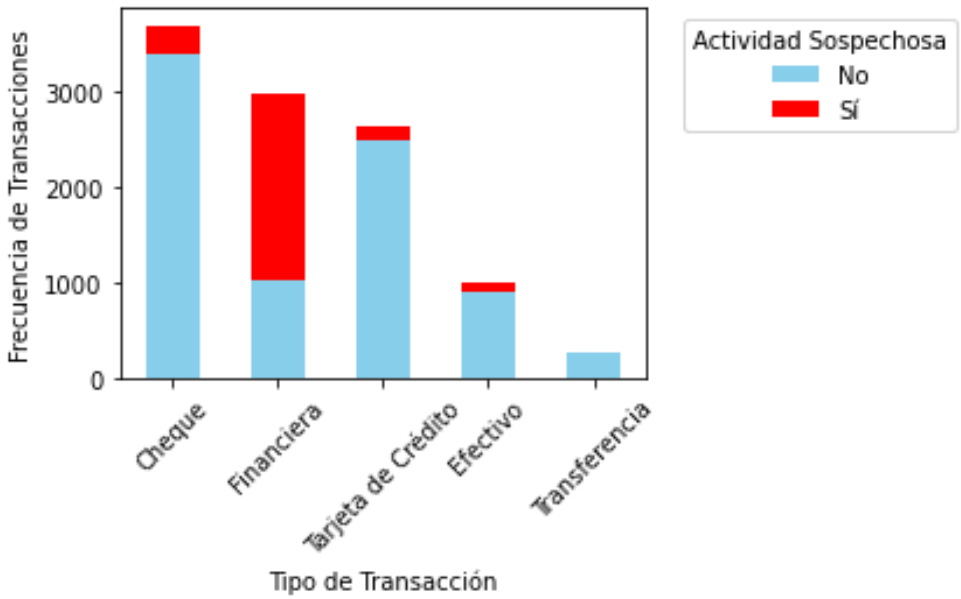
Nota. AMLSim-IBM

Elaboración propia.

Por otro lado, en la figura 23 se muestra el análisis por tipo de transacción revela diferencias significativas notables en cuanto a la frecuencia de actividades sospechosas dónde destaca una fuerte preponderancia relativa en las transacciones del tipo financieras (65,7%), siendo esta la preferida por individuos que buscan llevar a cabo operaciones ilícitas. En contraste, que las otras formas de transacción como el efectivo (8,4%), cheque (7,8%), tarjetas de crédito (5,9%), que presentan menores en cuanto a las incidencias de actividad sospechosa.

Figura 23

Frecuencia de tipo de transacciones y actividades sospechosas



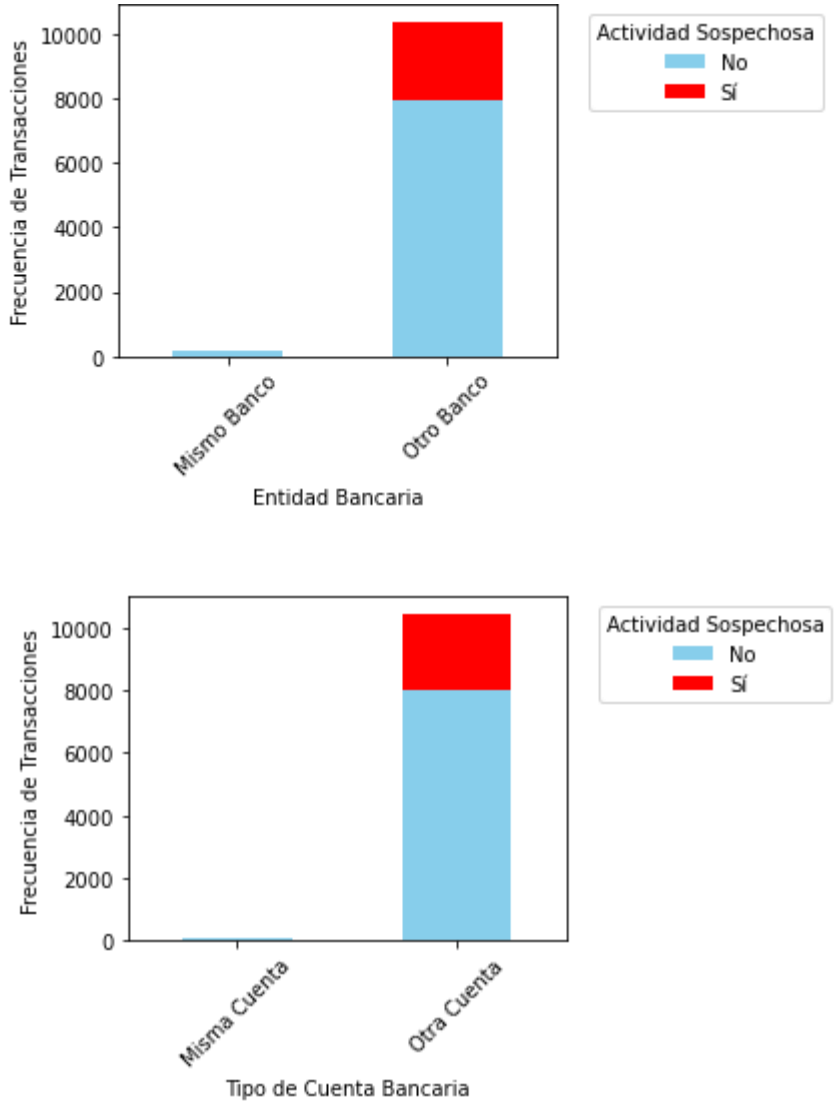
Nota. AMLSim-IBM

Elaboración propia.

En la figura 24 se observa que para el caso de la actividad sospechosa por entidad bancaria se puede apreciar claramente que la proporción relativa es de otro banco (23,6%) ya que manejan el volumen más alto de transacciones sospechosas, dónde este patrón puede ser útil para identificar qué tipo de instituciones financieras podrían necesitar fortalecer sus mecanismos de control y prevención de actividades ilícitas. De similar manera sucede con otra cuenta (23,7%), dónde la prevalencia de actividad sospechosa en ciertos tipos de cuentas puede señalar vulnerabilidades específicas o prácticas de monitoreo insuficientes para ciertas categorías de cuentas.

Figura 24

Frecuencia de transacciones por entidad / cuenta bancaria y actividades sospechosas



Nota. AMLSim-IBM

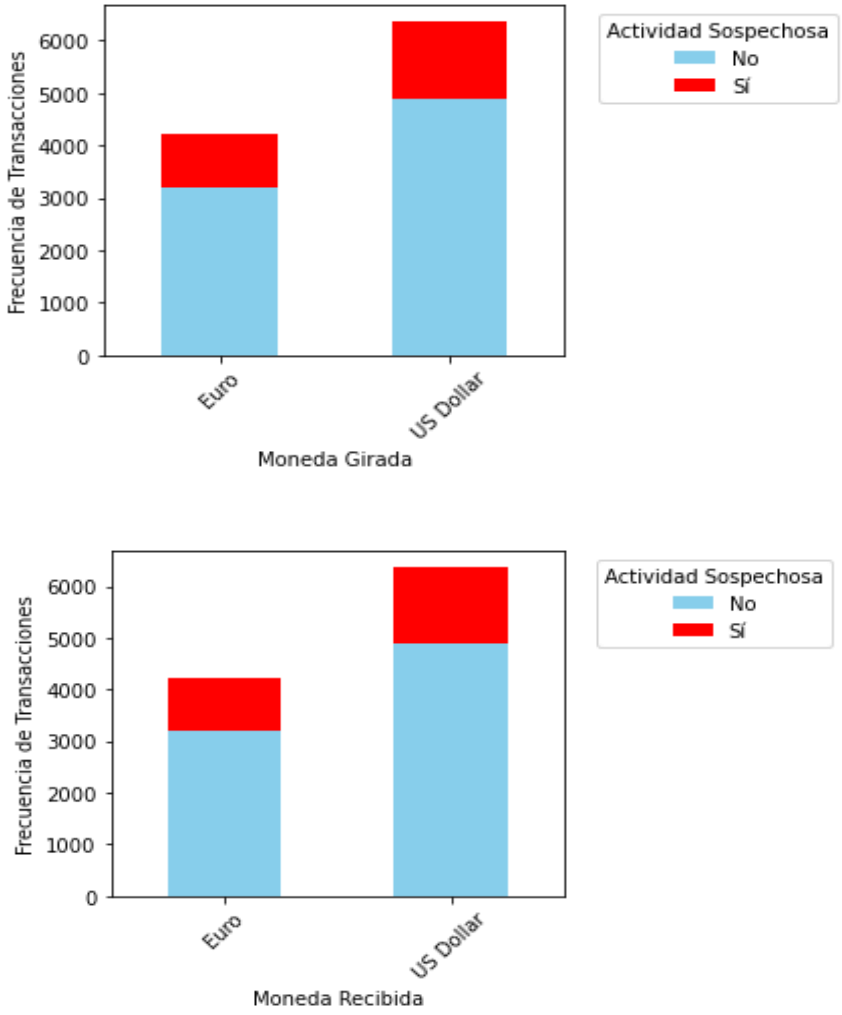
Elaboración propia.

En la figura 25 se muestra se evalúa la actividad sospechosa según el tipo de moneda involucrada en las transacciones, dónde se destaca que la moneda o divisa estadounidense (US Dollar) presenta una proporción significativa del 24,3% tanto en transacciones giradas como recibidas, lo que la convierte en la moneda más prevalente en actividades sospechosas en términos de volumen de actividades detectadas como sospechosas. Por otra

parte, aunque en menor frecuencia, el Euro también muestra una proporción notable de actividades sospechosas, con un 22,9%, subrayando también su relevancia en el contexto de transacciones ilícitas. Estos datos sugieren que el tipo de moneda, como el dólar estadounidense y el euro, podrían ser preferidas por actores ilícitos para realizar operaciones de lavado de dinero, posiblemente debido a su amplia aceptación y facilidad de movimiento en los mercados internacionales.

Figura 25

Frecuencia de transacciones por tipo de moneda girada /recibida y actividades sospechosas



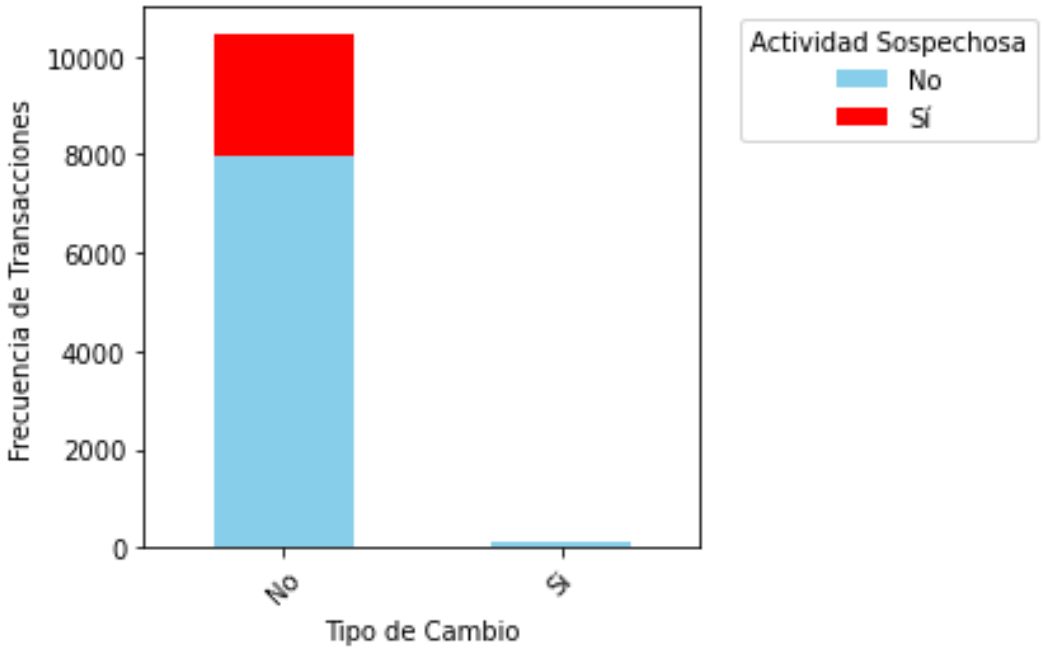
Nota. AMLSim-IBM

Elaboración propia.

En la figura 26 se visualiza la relación entre la presencia o ausencia del tipo de cambio en las transacciones en la incidencia de las actividades sospechosas. Se observa que las transacciones donde “No” se realiza un tipo de cambio presentan una prevalencia del 23,7% en actividades sospechosas. Mientras que, con las transacciones que “Si” involucran un tipo de cambio, la incidencia de actividades sospechosas es insignificantes registrando casi 0%, este patrón sugiere que la mayoría de las transacciones sospechosas ocurren dentro del país analizado, utilizando la moneda local sin necesidad o preferencia de conversión a divisas extranjeras. Este hallazgo indica que las fluctuaciones o políticas de cambio de moneda no parecen influir notablemente en la detección de actividades ilícitas, lo que puede ofrecer insights importantes sobre cómo se estructuran las operaciones sospechosas, predominando aquellas que no requieren movimientos hacia otras divisas.

Figura 26

Frecuencia de transacciones por tipo de cambio y actividades sospechosas



Nota. AMLSim-IBM

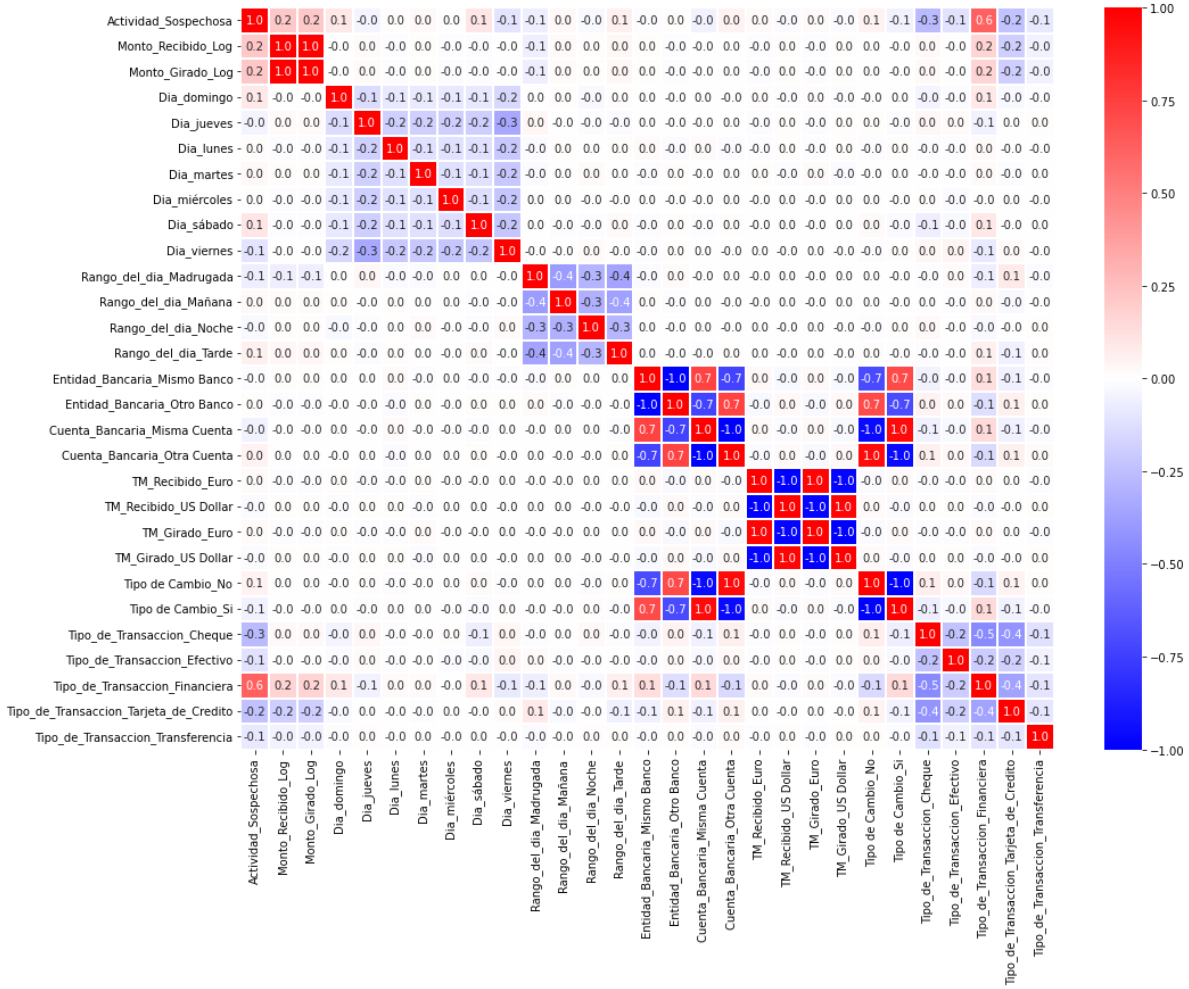
Elaboración propia.

- **ANÁLISIS DE CORRELACIÓN**

La matriz de correlación muestra las relaciones lineales entre todas las variables del conjunto de datos. A continuación, se presenta la figura 27, dónde se visualiza de manera detallada el valor de estas correlaciones, así como las más relevantes con respecto a la variable objetivo, y por ende a la casuística del estudio.

Figura 27

Matriz de correlaciones



Nota. AMLSim-IBM

Elaboración propia.

Hay que destacar que estas relaciones pueden ser útiles como línea base y simple para identificar patrones y tendencias en las transacciones bancarias que podrían indicar riesgo de actividades sospechosas, y pueden informar futuras investigaciones y modelos predictivos.

En tabla 4 de correlaciones se evidencian varias relaciones importantes entre las variables independientes (características) y Actividad Sospechosa (target). Dónde, las transacciones del tipo financieras y el monto girado y recibido tienen correlaciones positivas significativas con la actividad sospechosa, así como los días específicos del fin de semana (sábado y domingo) y el rango de horas de la tarde. Mientras que las transacciones del tipo (cheque y tarjeta de crédito) tienen correlaciones negativas significativas.

Tabla 4

Correlación de la variable objetivo (target) con las variables independientes

N	Variable	Correlación	Significancia	
		Actividad Sospechosa	p-value	
1	Tipo de transacción (financiera)	0.62	0.00	**
2	Monto girado (Log)	0.21	0.00	**
3	Monto recibido (Log)	0.21	0.00	**
4	Día sábado	0.10	0.00	**
5	Día domingo	0.09	0.00	**
6	Rango del día tarde	0.06	0.00	**
7	Tipo de cambio (No)	0.05	0.00	**
8	Cuenta bancaria (otra cuenta)	0.05	0.00	**
9	Rango del día mañana	0.03	0.00	**
10	Día martes	0.02	0.01	**
11	Tipo de moneda recibido (Euro)	0.02	0.09	n.s.
12	Tipo de moneda girado (Euro)	0.02	0.09	n.s.
13	Entidad bancaria (otro banco)	0.01	0.14	n.s.
14	Día lunes	0.01	0.18	n.s.
15	Día miércoles	0.01	0.54	n.s.

16	Entidad bancaria (mismo banco)	-0.01	0.14	n.s.
17	Tipo de moneda girada (US Dollar)	-0.02	0.09	n.s.
18	Tipo de moneda recibida (US Dollar)	-0.02	0.09	n.s.
19	Rango del día noche	-0.03	0.01	**
20	Día jueves	-0.04	0.00	**
21	Cuenta bancaria (misma cuenta)	-0.05	0.00	**
22	Tipo de cambio (Si)	-0.05	0.00	**
23	Rango del día madrugada	-0.07	0.00	**
24	Tipo de transacción (transferencia)	-0.09	0.00	**
25	Día viernes	-0.11	0.00	**
26	Tipo de transacción (efectivo)	-0.11	0.00	**
27	Tipo de transacción (tarjeta de crédito)	-0.24	0.00	**
28	Tipo de transacción (cheque)	-0.27	0.00	**

Nota. AMLSim-IBM

Elaboración propia.

4.3 FASE 2: PREPARACIÓN Y PREPROCESAMIENTOS DE LOS DATOS

Durante la Fase 1 “Ingesta y comprensión de los datos” en el apartado “Análisis univariado”, se observó que las variables cuantitativas “Monto Girado” y “Monto Recibido” presentaban una elevada dispersión y una distribución sesgada a la derecha. Esta condición es común en datos financieros donde existen transacciones de montos significativamente altos que afectan la estabilidad de los modelos predictivos.

Con la finalidad de reducir esta dispersión y atenuar el impacto de los valores extremos se aplicó una transformación logarítmica a ambas variables.

Esta técnica estadística permite normalizar la distribución de los datos haciendo que sean más simétricos y facilitando el desempeño y la precisión de los algoritmos de aprendizaje automático aplicados posteriormente.

En la figura 28 se presentan los estadísticos descriptivos posteriores a la transformación, mientras que la figura 29 muestra los histogramas de las variables transformadas evidenciando una distribución más simétrica.

Finalmente, la figura 30 ilustra los diagramas de cajas que demuestran la reducción de la variabilidad y la presencia controlada de valores atípicos.

Con esta transformación se logra una base de datos más adecuada para el entrenamiento de modelos predictivos, garantizando análisis más precisos y fiables en la detección temprana de transacciones sospechosas de lavado de activos.

Figura 28

Estadísticos descriptivos de las variables cuantitativas: monto recibido y girado transformadas

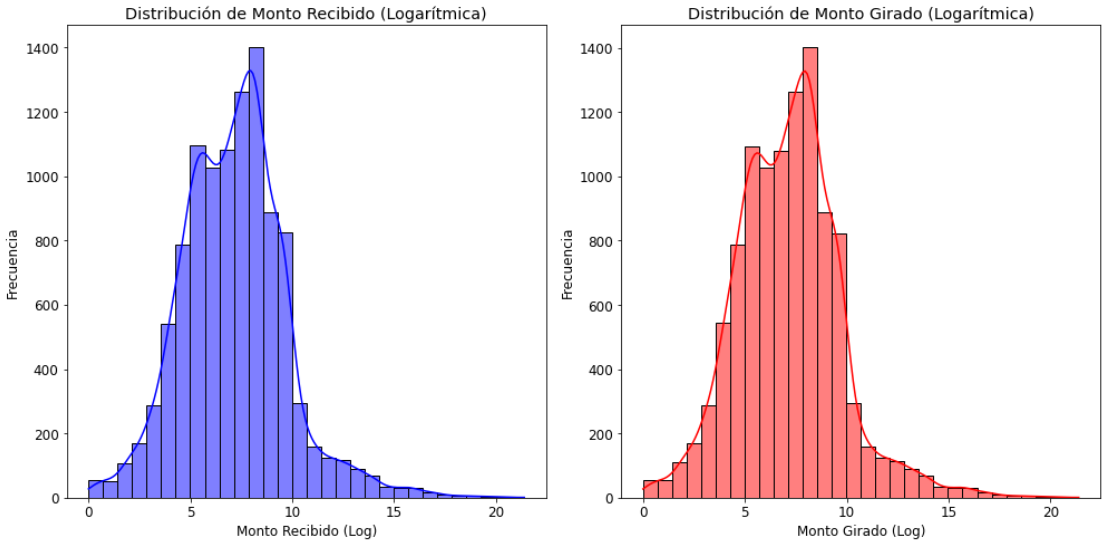
	Monto_Recibido_Log	Monto_Girado_Log
count	10568.000000	10568.000000
mean	7.162073	7.162031
std	2.565417	2.565434
min	0.009950	0.009950
25%	5.426117	5.427018
50%	7.180112	7.180523
75%	8.609515	8.609515
max	21.379696	21.379696

Nota. AMLSim-IBM

Elaboración propia.

Figura 29

Histogramas de las variables monto girado y recibido transformado

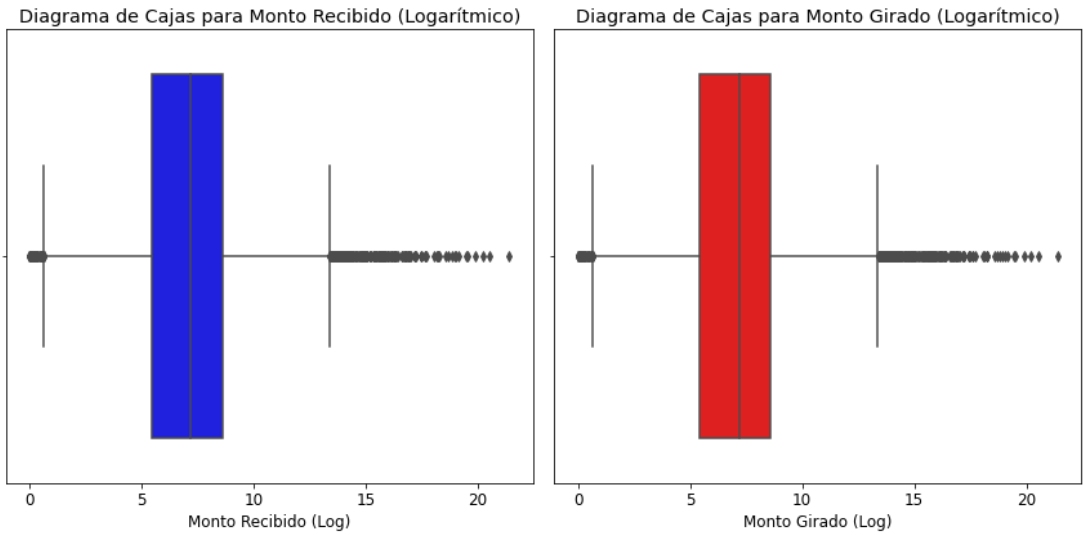


Nota. AMLSim-IBM

Elaboración propia.

Figura 30

Diagrama de cajas de las variables monto girado y recibido transformado



Nota. AMLSim-IBM

Elaboración propia.

4.4 FASE 3: EXPERIMENTACIÓN Y SELECCIÓN DE MODELOS

La presente fase tiene como objetivo identificar el modelo predictivo con mayor capacidad para la detección temprana de transacciones sospechosas de lavado de activos. Para ello se aplicó un proceso sistemático inspirado en las buenas prácticas de ingeniería de aprendizaje automático descritas por Probst, Wright y Boulesteix (2019), combinando: (i) Definición de los algoritmos candidatos, (ii) Diseño experimental, (iii) Hiperparámetros y justificación.

a. Selección de algoritmos candidatos

Se incluyeron siete familias algorítmicas con sesgos inductivos distintos, a fin de cubrir tanto modelos lineales como no lineales:

- **Regresión Logística**: empleada como baseline interpretable en problemas binarios, con coeficientes que permiten analizar la contribución de cada característica (Hosmer et al., 2013)
- **Árbol de Decisión**: genera reglas de decisión jerárquicas comprensibles y facilita la extracción de conocimiento (Quinlan, 1986).
- **Random Forest**: ensamble bagging que reduce la varianza mediante el agregado de árboles construidos sobre subconjuntos aleatorios (Breiman, 2001)
- **Support Vector Machine (SVM)**: maximiza el margen entre clases y, mediante *kernels*, modela fronteras no lineales en espacios de alta dimensión (Cortes & Vapnik, 1995).
- **K-Nearest Neighbors (KNN):** clasificador basado en proximidad sin supuestos paramétricos explícitos, útil como referencia flexible (Cover & Hart, 1967).
- **Red Neuronal Artificial (ANN)**: arquitectura multicapa capaz de aproximar funciones altamente no lineales (Haykin 2009).
- **XGBoost**: implementación optimizada de gradient boosting con regularización explicita, ampliamente validado en contextos tabulares (Chen & Guestrin, 2016)

Esta diversidad algorítmica permite mitigar el riesgo de dependencia a una única hipótesis funcional (Wolpert, 1996) y maximiza la probabilidad de hallar un modelo robusto.

b. Diseño experimental

El flujo experimental se estructuró para garantizar reproducibilidad y estimaciones imparciales del desempeño:

Partición de datos: Para el desarrollo de los modelos, es necesario dividir la información del conjunto de los datos en un 80% para el entrenamiento (train) y un 20% para la prueba (test). En la tabla 5 se observa la cantidad para cada conjunto de datos.

Tabla 5

Conjunto de datos para el entrenamiento y prueba

Conjunto de datos	Número de observaciones	Porcentaje (%)
Entrenamiento	8454	80
Prueba	2114	20
Total	**10568**	**100**

Nota. AMLSim-IBM

Elaboración propia.

- **Validación cruzada k-fold (k=5):** reduce la varianza de la estimación respecto a un simple *hold-out* y aprovecha eficientemente el tamaño muestral (Stone,1974)
- **Optimización de Hiperparámetros:** se aplicó Grid search para espacios moderados y Random Search cuando la dimensionalidad combinatoria era mayor, siguiendo la evidencia empírica de Bergstra y Bengio (2012) sobre su eficiencia.

- **Control de reproducibilidad:** fijación de la semilla aleatoria (random_state=42) y encapsulación en pipelines para evitar fugas de datos (VanderPlas,2016).
- **Gestión del desbalance:** la clase “sospechosa” representaba una minoría; por ello las métricas de optimización priorizadas fueron AUC-ROC y F1-Score, adecuadas para escenarios con distribución asimétrica (Saito & Rehmsmeier, 2015).

c. Hiperparámetros y justificación

A continuación, se detalla la configuración final seleccionada para cada algoritmo junto con su fundamentación teórica:

- **Regresión Logística**

  penalty=’l2’, C=1.0, solver=’lbfgs’, max_iter=1000

  La regularización L2 estabiliza los coeficientes y disminuye el sobreajuste, especialmente en presencia de variables correlacionadas (Ng, 2004). El valor C=1.0 ofrece un equilibrio sesgo-varianza razonable y ‘lbfgs’ es un optimizador eficiente para funciones log-likelihood suaves (Hastie et al., 2009)

- **Árbol de Decisión**

  Criterio=’gini’, max_depth=5, min_samples_split=10, min_samples_leaf=5

  Restringir la profundidad y el tamaño mínimo de nodos previene la generación de particiones demasiado específicas que inducen sobreajuste (Loh, 2011). El índice de Gini muestra rendimiento comparable a la entropía con menor coste computacional (Hastie et al., 2009).

- **Random Forest**

  n_estimators=100, max_depth=10, min_samples_split=5, min_samples_leaf=4

  Breiman (2001) señala que el error se estabiliza rápidamente conforme aumenta el número de árboles; 100 resulta suficiente

para equilibrar precisión y costo. Una profundidad moderada mejora la generalización y limita la correlación entre árboles (Biau & Scornet, 2016)

- **Support Vector Machine (SVM)**

  C=1.0, kernel='rbf', gamma='scale'

  El kernel RBF captura relaciones no lineales sin requerir parametrización manual compleja. Los valores iniciales (C=1, gamma='scale') son recomendados por guías prácticas y ajustan implícitamente la influencia de cada vector de soporte (Hsu, Chang & Lin, 2003).

- **K-Nearest Neighbors (KNN)**

  n_neighbors=5, metric='minkowski',p=2,weights='uniform'

  Cover y Hart (1967) demostraron que, para tamaños muestrales grandes, pocos vecinos (k pequeño) mantienen una baja tasa de error asintótico. El uso de distancia Euclídea (p=2) es estándar en datos numéricos transformados.

- Red Neuronal Artificial

  Hidden_layer_sizes=(50,30,10), activation='relu', solver='adam', alpha=0.001, max_iter=300

  La función ReLU mitiga el problema del gradiente desvanecido y acelera la convergencia (Glorot & Bengio, 2011). El optimizador Adam combina momentos adaptativos, logrando convergencia estable en dominios tabulares (Kingma & Ba, 2015). La regularización L2 (Alpha) reduce la parametrización.

- **XGBoost**

  n_estimators=100, max_depth=6, learning_rate=0.1, subsample=0.8, colsample_bytree=0.8, gamma=0, reg_lambda=1

  Chen y Guestrin (2016) proponen esta configuración como punto de partida: la tasa de aprendizaje moderada (0.1) combinada con 100 iteraciones ofrece suficiente capacidad de corrección

incremental. Los coeficientes de muestreo (subsample, colsample_bytree) introducen estocasticidad que disminuye el sobreajuste, mientras que la regularización (reg_lambda) penaliza la complejidad del ensamble (Brownlee, 2019).

En la tabla 6 se muestra un resumen de los algoritmos con sus Hiperparámetros con sus respectivas justificaciones.

Tabla 6

Resumen de las configuraciones de los algoritmos

Modelo	Hiperparámetros Finales	Justificación resumida
Regresión Logística	L2, C=1.0, lbfgs	Regularización para evitar sobreajuste (Ng, 2004).
Árbol de Decisión	depth=5, min_split=10, min_leaf=5	Control de complejidad (Loh, 2011).
Random Forest	100 árboles, depth=10	Asegurar la diversidad y la estabilidad (Breiman, 2001).
SVM (RBF)	C=1, gamma=scale	Separación no lineal eficiente (Hsu et al., 2003).
KNN	k=5, Euclídea	Suavizar efectos de valores atípicos (Cover & Hart, 1967).
ANN	(50,30,10), ReLU, Adam, α=0.001	Arquitectura en embudo (Kingma & Ba, 2015).
XGBoost	100 est., depth=6, lr=0.1, subsample=0.8	Equilibrio entre precisión y tiempo (Chen & Guestrin, 2016).

Nota: AMLSim-IBM

Elaboración propia

4.5 FASE 4: VALIDACIÓN Y EVALUACIÓN DE MODELOS

El objetivo de esta fase es evaluar el rendimiento de las predicciones del modelo utilizando métricas como la Exactitud (*Accuracy*), la Precisión, la Sensibilidad (*Recall*), el F1-score, además de determinar la curva ROC y el AUC (*Area Under the Curve*). Esto proporcionará una referencia sobre la calidad del ajuste del modelo. Posteriormente, se compararon los indicadores de estas métricas en todos los modelos analizados para determinar cuál es el mejor en la detección de transacciones sospechosas en cuentas bancarias relacionadas con el lavado de activos.

4.5.1 Modelo por Regresión Logística

Presentamos la evaluación del modelo de regresión logística diseñado para la detección temprana de transacciones o actividades sospechosas de lavado de activos en instituciones financieras.

El modelo entrenado mostró un desempeño robusto y confiable, como se resume en la tabla 7. La Accuracy del modelo en el conjunto de prueba fue del 89%, lo que indica una alta exactitud en la clasificación de las transacciones. Además, la precisión, recall y el F1-Score de la prueba fueron del 77% en estos casos respectivamente, demostrando un buen equilibrio en la identificación de transacciones sospechosas.

Tabla 7

Métricas del modelo Regresión Logística entrenado con la data de prueba

Clase	Precision	Recall	F1-Score
0	0,93	0,92	0,93
1	0,77	0,77	0,77

Modelo de Regresión Logística	Accuracy	0,89
	AUC	0,867

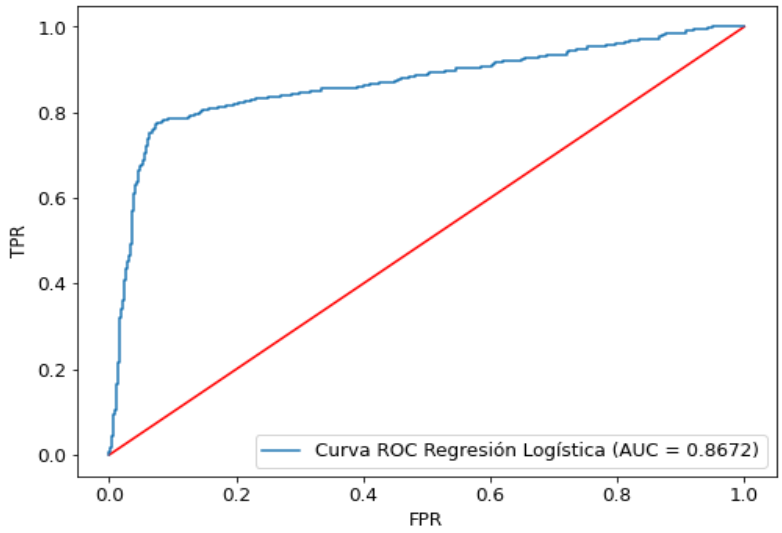
Nota. AMLSim-IBM

Elaboración propia.

Adicionalmente, en la figura 31 se determina el área bajo la curva ROC (AUC-ROC) resultando un valor del 86,7% reflejando una excelente capacidad del modelo para diferenciar las clases de actividades que son y no son sospechosas.

Figura 31

Curva ROC del modelo de Regresión Logística



Nota: AMLSim-IBM

Elaboración propia

En conclusión, el modelo de regresión logística ha demostrado ser efectivo y robusto para la detección de transacciones sospechosas. La consistencia en el desempeño entre los conjuntos de entrenamiento y prueba sugiere que el modelo generaliza bien a nuevos datos.

4.5.2 Modelo por Support Vector Machine (SVM)

Se analiza el rendimiento del modelo SVM (Support Vector Machine), implementado para la identificación de transacciones o comportamientos potencialmente asociados al lavado de activos en instituciones financieras. El desempeño del SVM se presenta como un buen modelo y efectivo, tal como se detalla en la tabla 8, el Accuracy, alcanzó un 87%, mostrando una buena

capacidad de clasificación general de las transacciones evaluadas. Además, para la clase de transacciones consideradas sospechosas, el modelo logró una Precisión de 72%, con un Recall significativamente superior con el 78%, lo que condujo a un F1-Score de 75%, aunque hay valores que son ligeramente inferiores comparativamente hablando con las métricas del modelo de Regresión Logística, estas aún demuestran una capacidad aceptable del modelo para detectar actividades potencialmente ilícitas.

Tabla 8

Métricas del modelo SVM entrenado con la data de prueba

Clase	Precision	Recall	F1-Score
0	0,93	0,90	0,92
1	0,72	0,78	0,75
Modelo SVM		Accuracy	0,87
		AUC	0,843

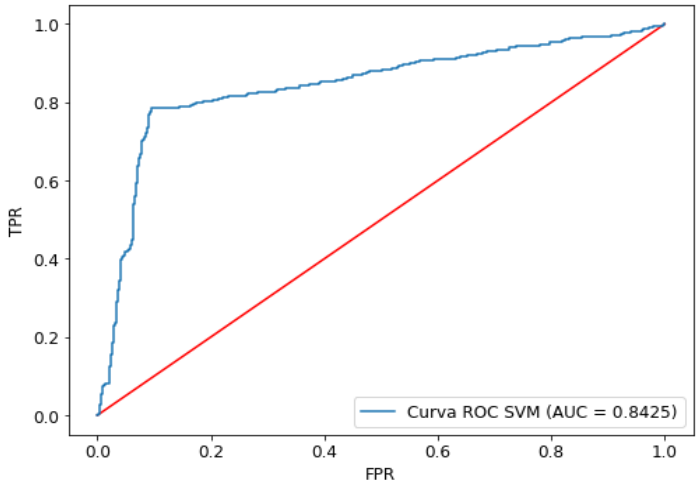
Nota. AMLSim-IBM

Elaboración propia.

Adicionalmente, en la figura 32 se determina el área bajo la curva ROC (AUC-ROC) resultando un valor del 84,3% que refuerza el rendimiento del modelo SVM para discriminar entre las clases de manera efectiva, aunque con una ligera reducción en comparación con la regresión logística.

Figura 32

Curva ROC del modelo Support Vector Machine (SVM)



Nota. AMLSim-IBM

Elaboración propia.

En conclusión, el modelo SVM ha demostrado capacidad y eficiencia en la identificación de transacciones sospechosas, con un rendimiento aceptable tanto en precisión como en recall. Aunque la exactitud general y el AUC son ligeramente inferiores al modelo de regresión logística, el SVM ofrece un balance adecuado entre la detección de casos que son y no son sospechosos.

4.5.3 Modelo por K Nearest Neighbors (KNN)

Ahora se analiza el desempeño del modelo K Nearest Neighbors (KNN) aplicado a la detección temprana de transacciones sospechosas en el contexto de instituciones financieras. El modelo KNN demostró una actuación consistente y eficaz, como se observa en la tabla 9, el Accuracy alcanzó el 89%, reflejando una excelente habilidad para clasificar correctamente las transacciones evaluadas. Para la clase de transacciones sospechosas, KNN alcanzó una precisión del 80% y un recall del 72%, resultando en un F1-Score de 76%, lo que indica una capacidad considerable para detectar actividades

potencialmente ilícitas, hay que destacar que hay indicadores con un margen de mejora.

Tabla 9

Métricas del modelo KNN entrenado con la data de prueba

Clase	Precision	Recall	F1-Score
0	0,91	0,94	0,93
1	0,80	0,72	0,76
Modelo KNN		Accuracy	0,89
		AUC	0,853

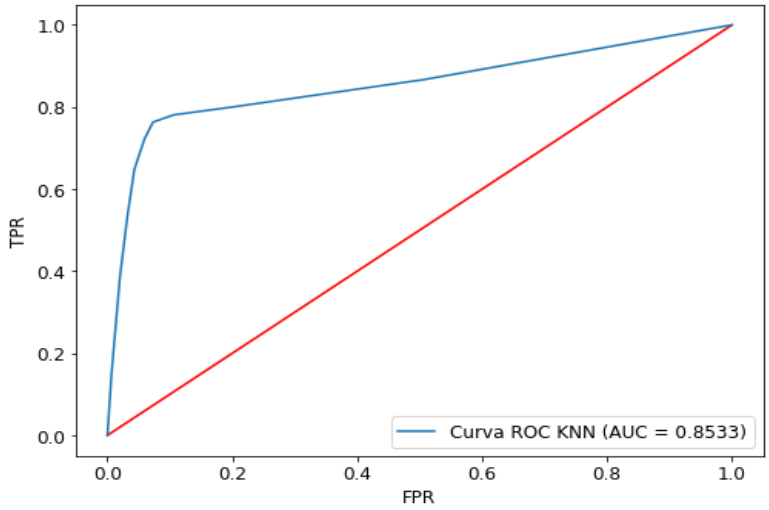
Nota. AMLSim-IBM

Elaboración propia.

Adicionalmente, en la figura 33 se determina el área bajo la curva ROC (AUC-ROC) resultando un valor del 85,3% que subraya la competencia del modelo para discriminar entre clases sospechosas y no sospechosas de manera efectiva, mostrando una robustez comparable con los otros modelos analizados.

Figura 33

Curva ROC del modelo K Nearest Neighbors (KNN)



Nota. AMLSim-IBM

Elaboración propia.

4.5.4 Modelo por Artificial Neural Network (ANN)

Se contempla el análisis del modelo de red neuronal artificial (ANN), diseñado para mejorar la detección de transacciones sospechosas de lavado de activos en instituciones financieras. El modelo ANN exhibió un desempeño sobresaliente, como se refleja en la tabla 10, logrando un Accuracy del 89%, indicativo de su alta capacidad para clasificar adecuadamente las transacciones dentro del conjunto de prueba. En particular, para transacciones no sospechosas (clase 0), el modelo alcanzó una precisión del 92% y un recall del 95%, resultando en un F1-Score de 93%, demostrando una eficacia notable en la identificación de transacciones que no serían sospechosas. En contraste, para las transacciones sospechosas (clase 1), la precisión fue del 81% con un recall del 74%, y un F1-Score de 77%, lo cual, aunque es ligeramente inferior en comparación con la clase 0, sigue siendo robusto y muestra un rendimiento adecuado en la detección de actividades potencialmente fraudulentas.

Tabla 10

Métricas del modelo ANN entrenado con la data de prueba

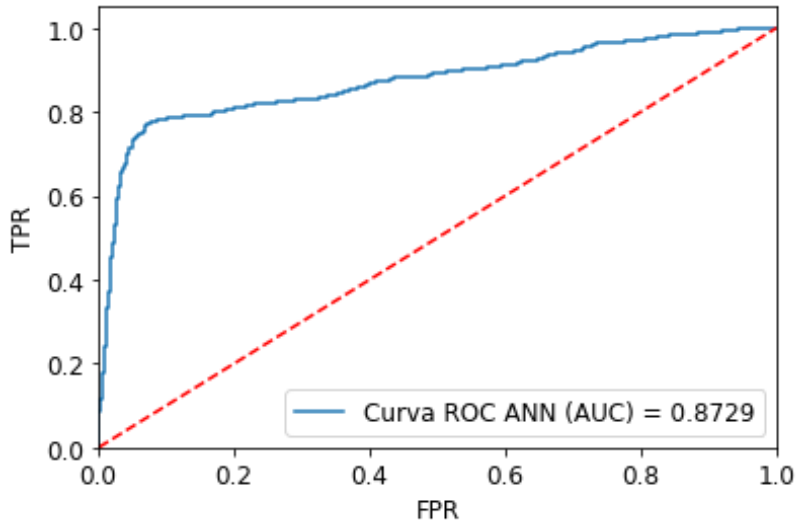
Clase	Precision	Recall	F1-Score
0	0,92	0,95	0,93
1	0,81	0,74	0,77
Modelo ANN		Accuracy	0,89
		AUC	0,873

Nota. Elaboración propia.

Adicionalmente, en la figura 34 se determina el área bajo la curva ROC (AUC-ROC) resultando un valor del 87,3% que confirma la capacidad del modelo ANN para diferenciar eficazmente entre clases, proporcionando una base y detección aún más robusta que los modelos anteriores por lo que sería ideal su uso en estos entornos de vigilancia financiera.

Figura 34

Curva ROC del modelo Artificial Neural Network (ANN)



Nota. AMLSim-IBM

Elaboración propia.

En conclusión, el modelo ANN ha validado su efectividad y robustez en la identificación de transacciones sospechosas, con niveles de Accuracy, Precisión, F-Score y AUC más altos que los modelos anteriores. Hay que destacar que a pesar de presentar retos inherentes a la complejidad de las redes neuronales, sus resultados predictivos indican un potencial significativo para futuras mejoras y ajustes más detallados en la casuística de estudio.

4.5.5 Modelo por Decision Tree

Se evalúa el modelo de árbol de decisión (Decision Tree) aplicado a la detección de transacciones sospechosas en instituciones financieras. El modelo de árbol de decisión mostró un rendimiento robusto y eficiente, como se observa en la tabla 11. El Accuracy, alcanzó el 90%, lo que indica una excelente capacidad de clasificación correcta de las transacciones evaluadas. Para la clase de transacciones no sospechosas (clase 0), el modelo logró una precisión de 92% y un recall de 94%, con un F1-Score de 93%, destacando su habilidad para identificar correctamente las transacciones legítimas. Por otro lado, para las transacciones sospechosas (clase 1), la precisión fue del 81% con un recall del 75%, y un F1-Score de 78%, demostrando una capacidad eficaz para señalar transacciones potencialmente fraudulentas, aunque con margen de mejora en la identificación.

Tabla 11

Métricas del modelo Decision Tree entrenado con la data de prueba

Clase	Precision	Recall	F1-Score
0	0,92	0,94	0,93
1	0,81	0,75	0,78
Modelo	Decision Tree	Accuracy	0,90
		AUC	0,872

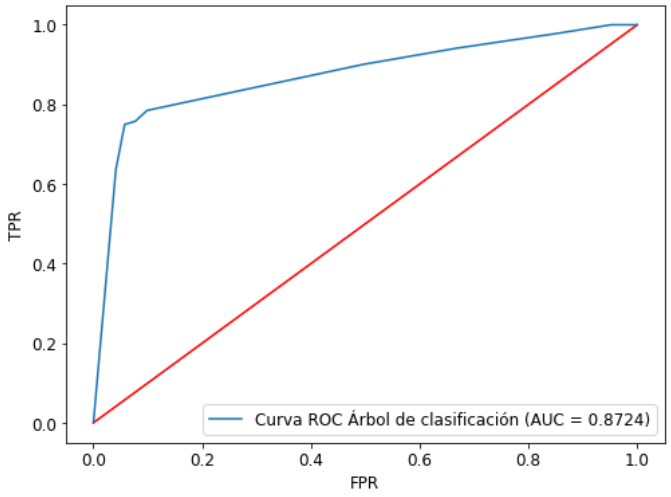
Nota. AMLSim-IBM

Elaboración propia.

Adicionalmente, en la figura 35 se determina el área bajo la curva ROC (AUC-ROC) resultando un valor del 87,2% que enfatiza la competencia del modelo Decision Tree para diferenciar entre clases de manera efectiva, ofreciendo una solución prometedora para la detección de actividades sospechosas en entornos financieros.

Figura 35

Curva ROC del modelo Decision Tree



Nota. AMLSim-IBM

Elaboración propia.

En conclusión, el modelo de árbol de decisión ha demostrado ser aún más efectivo y confiable en la identificación de transacciones sospechosas comparativamente hablando que los modelos previos, con un rendimiento que respalda su uso en aplicaciones de vigilancia financiera.

4.5.6 Modelo por Random Forest

Este análisis se centra en el modelo Random Forest, utilizado para la identificación de transacciones sospechosas de lavado de activos en instituciones financieras. El modelo Random Forest demostró un desempeño excelente, como se refleja en la tabla 12, con un Accuracy del 90%, el modelo exhibe una alta eficacia en la clasificación de las transacciones. Para las transacciones no sospechosas (clase 0), alcanzó una precisión del 93% y un recall del 94%, resultando en un F1-Score de 93%, lo que evidencia su capacidad para identificar correctamente las transacciones legítimas o que no son sospechosas de manera efectiva. Para las transacciones sospechosas (clase 1), la precisión fue del 80% y el recall del 77%, con un F1-Score de 78%, demostrando una competencia sólida para detectar transacciones potencialmente ilícitas.

Tabla 12

Métricas del modelo Random Forest entrenado con la data de prueba

Clase	Precision	Recall	F1-Score
0	0,93	0,94	0,93
1	0,80	0,77	0,78

Modelo	Random	Accuracy	0,90
Forest		AUC	0,875

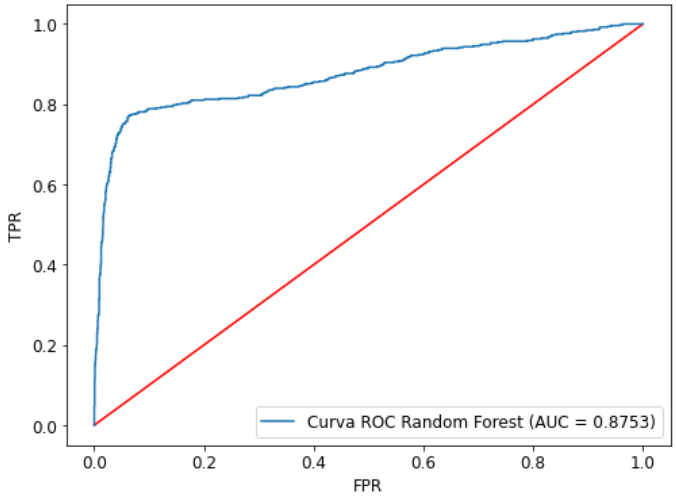
Nota. AMLSim-IBM

Elaboración propia.

Adicionalmente, en la figura 36 se determina el área bajo la curva ROC (AUC-ROC) resultando un valor del 87,5% que refuerza la habilidad del modelo para discriminar entre clases de manera efectiva, situando al Random Forest como una herramienta altamente robusta y confiable en el contexto de vigilancia financiera.

Figura 36

Curva ROC del modelo Random Forest



Nota. AMLSim-IBM

Elaboración propia.

En conclusión, el modelo Random Forest ha probado ser un instrumento efectivo y aún más potente que los modelos previos para la identificación de transacciones sospechosas, con un rendimiento que justifica su implementación en entornos de vigilancia financiera. Sus altas métricas de Accuracy, F1-Score y AUC, subrayan su utilidad práctica y trazan un camino más propicio en la implementación del modelo para futuras mejoras y ajustes de esta.

4.5.7 Modelo por XGBoost

Finalmente, se presenta el análisis del modelo XGBoost (Extreme Gradient Boosting), implementado para la detección de transacciones sospechosas en instituciones financieras. Es importante destacar que XGBoost emplea árboles de decisión en secuencia, mejorando gradualmente el rendimiento del modelo al corregir los errores de predicciones anteriores. Este enfoque ha sido entrenado para diferenciar de manera eficaz entre transacciones normales y potencialmente ilícitas. El modelo XGBoost ha mostrado un excelente rendimiento, destacando entre todos los modelos analizados y evaluados hasta el momento. Como se observa en la tabla 13 el Accuracy del modelo resultó ser del 90%, evidenciando su eficiencia en la clasificación precisa de transacciones. En el caso de las transacciones no sospechosas (clase 0), el modelo alcanzó una impresionante precisión del 92% y un recall del 96%, lo cual se traduce en un F1-Score de 94%, mostrando una habilidad superior para identificar transacciones legítimas. Para las transacciones sospechosas (clase 1), logró una precisión del 84% y un recall del 73%, con un F1-Score de 78%, indicando una efectividad robusta en la detección de actividades ilícitas.

Tabla 13

Métricas del modelo XGBoost entrenado con la data de prueba

Clase	Precision	Recall	F1-Score
0	0,92	0,96	0,94
1	0,84	0,73	0,78
Modelo XGBoost		Accuracy	0,90
		AUC	0,880

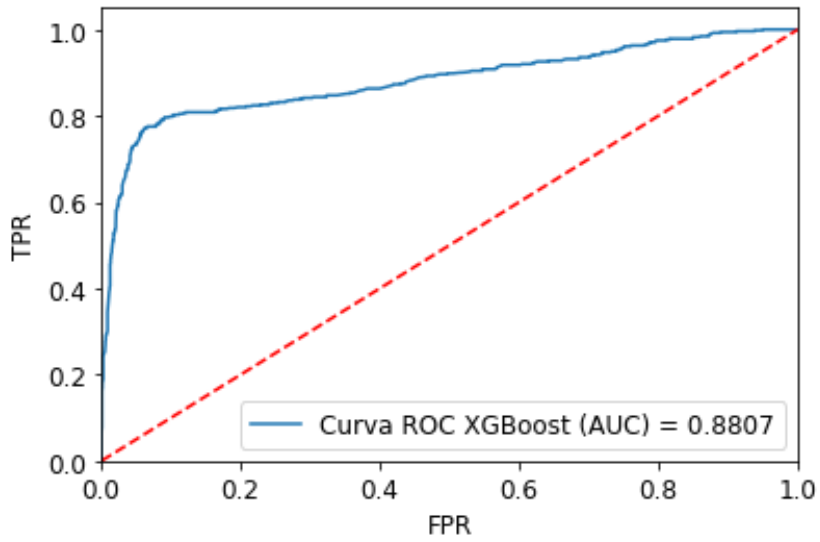
Nota. AMLSim-IBM

Elaboración propia.

Adicionalmente, en la figura 37 se determina el área bajo la curva ROC (AUC-ROC) resultando un valor del 88,0% es el más alto registrado entre los modelos evaluados, subrayando la capacidad sobresaliente de XGBoost para diferenciar entre clases con gran precisión.

Figura 37

Curva ROC del modelo XGBoost



Nota. AMLSim-IBM

Elaboración propia.

En conclusión, el modelo XGBoost no solo ha validado su eficacia y precisión en la detección de transacciones sospechosas, sino que también ha demostrado ser el más efectivo de todos los modelos evaluados, ofreciendo un equilibrio óptimo entre la detección de casos que no son sospechosos y sospechosos, dónde esto lo posiciona como una herramienta o técnica de aprendizaje automático altamente recomendable para la implementación en sistemas de vigilancia financiera, con un gran potencial para futuras optimizaciones.

4.6 FASE 5: DESPLIEGUE E IMPLEMENTACIÓN

Esta fase corresponde a la puesta en producción del modelo desarrollado, integrándose en un entorno real mediante una API, un servicio en la nube o algún sistema que permita su uso por parte de los usuarios o aplicaciones. Sin embargo, esta fase no será abordada en la presente investigación, ya que el modelo propuesto se desarrolla con fines académicos y de validación experimentar, sin contemplar su integración en un sistema de producción o infraestructura tecnológica institucional

4.7 FASE 6: MONITOREO Y MANTENIMIENTO

El monitoreo continuo del rendimiento del modelo en producción permite detectar desviaciones, degradación en la calidad de las predicciones o cambios en el comportamiento de los datos (data drift). No obstante, esta fase no incluye en el alcance del presente trabajo, dado que el modelo no será desplegado y, por lo tanto, no se requiere implementar mecanismos de monitoreo, reentrenamiento o mantenimiento periódico.

CAPÍTULO V

ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

5.1 ANÁLISIS DE LOS RESULTADOS

5.1.1 Comparación de los modelos implementados

En la Tabla 14 se presentan los resultados comparativos de desempeño de los modelos de aprendizaje automático implementados en la detección de transacciones sospechosas de lavado de activos. Las métricas consideradas incluyen Accuracy, Precision, Recall, F1-Score, Área bajo la curva ROC (AUC) y el coeficiente de Gini, todos ellos indicadores para evaluar modelos de clasificación binaria en problemas financieros (Powers,2011).

De acuerdo con los resultados, **el modelo XGBoost como la mejor alternativa** al obtener un Accuracy del 90%, una precisión del 84%, un AUC de 88% y un coeficiente de Gini de 76%. El AUC elevado refleja la alta capacidad del modelo para diferenciar entre transacciones sospechosas y no sospechosas, lo cual es clave en contextos de detección de fraudes y lavado de activo, donde la capacidad discriminativa del modelo es crucial (Fawcett, 2006)

Comparativamente, aunque modelos como Random Forest y Redes Neuronales Artificiales mostraron también un Accuracy del 90%, sus niveles de Precision, Recall y F1-Score fueron inferiores o similares, pero con un menor AUC y coeficiente de Gini, lo que indica un menor poder discriminativo general. Por ejemplo, Random Forest alcanzó un AUC de 87.5% frente al 88% de XGBoost, mientras que la Red Neuronal obtuvo un AUC de 85.7%.

Es importante señalar que el modelo XGBoost se caracteriza por su capacidad para gestionar grandes volúmenes de datos, manejar relaciones no lineales y controlar el sobreajuste mediante técnicas como el regularization L1 y L2 (Chen & Guestrin, 2016). Estas características lo convierten en un algoritmo altamente efectivo en contextos financieros.

En consecuencia, considerando el equilibrio logrado entre todas las métricas, así como el respaldo de la literatura que posiciona a XGBoost como uno de los algoritmos más robustos y eficaces para tareas de clasificación binaria (Nielsen, 2016; Chen & Guestrin, 2016), se determinó que este modelo sería el seleccionado para la interpretación de variables y la evaluación de impacto en la detección temprana de transacciones sospechosas de lavado de activos.

Tabla 14

Métricas de desempeño de los modelos de aprendizaje automático para la detección de transacciones sospechosas

Modelo	Accuracy	Precision	Recall	F1-Score	AUC	Gini
Regresión Logística	0,89	0,77	0,77	0,77	0,867	0,734
Support Vector Machine	0,87	0,72	0,78	0,75	0,843	0,686
K Nearest Neighbors	0,89	0,80	0,72	0,76	0,853	0,706
Artificial Neural Network	0,89	0,81	0,74	0,77	0,873	0,746
Decision Tree	0,90	0,81	0,75	0,78	0,872	0,744
Random Forest	0,90	0,80	0,77	0,78	0,875	0,750
XG Boost	0,90	0,84	0,73	0,78	0,880	0,760

Nota. AMLSim-IBM

Elaboración propia.

5.1.2 Evaluación de las métricas de XGBoost

Para evaluar el rendimiento del modelo XGBoost en la detección de transacciones sospechosas, se utilizaron métricas estándar de clasificación binaria, ampliamente reconocidas en la literatura científica y en aplicaciones prácticas de detección de fraude. Estas métricas permiten medir el equilibrio entre la identificación efectiva de casos positivos (transacciones sospechosas) y la reducción de errores de clasificación.

Las métricas utilizadas fueron las siguientes:

- **Accuracy:** Indica la proporción total de predicciones correctas (tanto sospechosas como no sospechosas) sobre el total de transacciones analizadas. Aunque en problemas con clases desbalanceadas puede ser engañosa, sigue siendo una métrica de referencia general. El modelo obtuvo una exactitud de **90%**, lo que muestra un buen rendimiento general.
- **Precisión (Precision):** Indica la proporción de transacciones clasificadas como sospechosas que realmente lo eran. Es especialmente relevante en contextos donde los falsos positivos representan una carga operativa significativa. En este estudio, el modelo obtuvo una precisión del **84%**, lo que evidencia una alta exactitud en la predicción de casos verdaderamente sospechosos.
- **Sensibilidad o Tasa de Verdaderos Positivos (Recall):** Mide la capacidad del modelo para identificar correctamente todas las transacciones sospechosas presentes en los datos. Dado que en problemas de lavado de activos es prioritario minimizar los falsos negativos (casos sospechosos que pasan desapercibidos), esta métrica es crítica. El modelo logró un recall del **73%**, indicando una cobertura amplia de los casos relevantes.
- **F1-Score:** Es la media armónica entre la precisión y el recall, y se emplea como una métrica equilibrada cuando es importante considerar tanto la exactitud como la cobertura. El modelo obtuvo un F1-Score de **78%**, lo cual refleja un desempeño sólido y balanceado en ambos aspectos.

- **Área bajo la Curva ROC (AUC):** Evalúa la capacidad del modelo para distinguir entre clases positivas (sospechosas) y negativas (no sospechosas), independientemente del umbral de decisión. Un valor de **88%** indica que el modelo tiene una excelente habilidad discriminativa, superando el umbral comúnmente aceptado de 80% para modelos confiables en contextos de riesgo.
- **Gini**: Es una transformación del AUC que también mide la capacidad del modelo para distinguir entre clases. Se obtuvo un valor del **76%** lo que indica que el modelo posee una capacidad muy alta de separación entre transacciones sospechosas y no sospechosas. Este índice es especialmente utilizado en sectores financieros como medida de poder predictivo.

Estas métricas fueron calculadas a partir de los datos de validación, empleando técnicas de validación cruzada para garantizar la estabilidad de los resultados. La combinación de un alto AUC, elevada precisión y sensibilidad posiciona al modelo XGBoost como una solución eficaz y robusta para la detección temprana de transacciones con patrones sospechosos.

Tabla 15

Métricas del modelo XGBoost

Modelo	Accuracy	Precision	Recall	F1-Score	AUC	Gini
XG Boost	90%	84%	73%	78%	88%	76%

Nota. AMLSim-IBM

Elaboración propia.

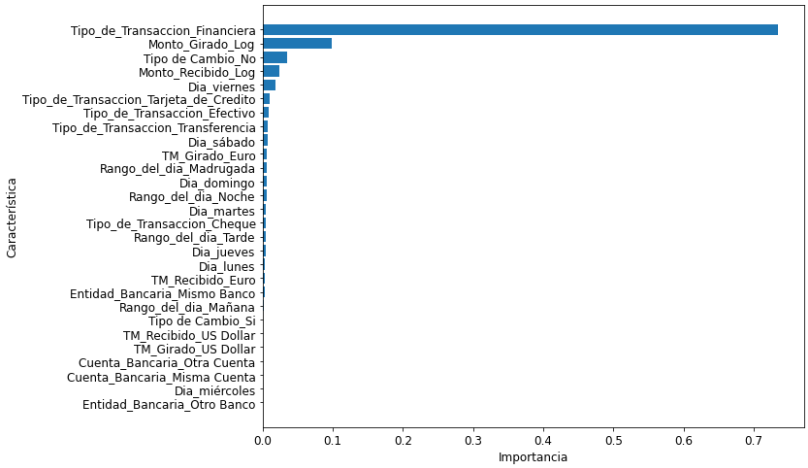
A continuación, se presenta la evaluación de la importancia relativa de las variables o características que componen el conjunto de datos, utilizando el mejor modelo identificado en la investigación: XGBoost. La determinación de la importancia de las variables permite identificar cuáles son los factores que mayor influencia ejercen en la predicción de transacciones sospechosas.

Según el modelo XGBoost, la variable con mayor peso fue el tipo de transacción financiera, seguida por el monto girado y el monto recibido (ambos en su versión transformada logarítmica), así como el tipo de cambio. Estos resultados coinciden con la literatura previa que señala que las características transaccionales y financieras son determinantes clave en la identificación de comportamientos atípicos o ilícitos (Delamaire et al., 2009; Chen & Guestrin, 2016). Asimismo, otras variables como el tipo de transacción con tarjeta de crédito, el tipo de transacción en efectivo, y la franja horaria también demostraron aportar información relevante para la clasificación. Estos hallazgos reafirman la importancia de considerar no solo los montos y los tipos de transacción, sino también el contexto temporal y modalidades de pago, factores que pueden estar asociados a patrones típicos de actividades sospechosas (Correa et al., 2016).

En la Figura 38, se visualiza el ranking de importancia de las variables generadas por XGBoost, lo cual facilita la interpretación del modelo y proporciona una guía para futuras investigaciones o implementaciones en sistemas de monitoreo financiero.

Figura 38

Importancia de Variables según el modelo XGBoost



Nota. AMLSim-IBM

Elaboración propia.

a) Métricas del Sistema actual (pretest) vs métricas del XGBosst (postest)

Con el fin de analizar el potencial de mejora en la detección de transacciones sospechosas de lavado de activos, se realizó una evaluación comparativa entre el desempeño del sistema actual de monitoreo y el del modelo predictivo propuesto, basado en XGBoost. Esta comparación se organiza en dos escenarios: el pretest, que representa el desempeño del sistema actualmente en uso, y el postest, que refleja los resultados obtenidos mediante la aplicación del modelo XGBoost sobre una base de datos simulada. Es importante indicar que los datos analizados en cada caso no son exactamente las mismas**.** El sistema actual opera en un ambiente automatizado real, basado en reglas preestablecidas (rule-based system)**,** mientras que el modelo XGBoost fue evaluado utilizando datos generados artificialmente por el simulador AMLSim, desarrollado por IBM Research. A pesar de esta diferencia, la comparación se considera válida para evaluar el potencial que ofrece la incorporación de inteligencia artificial en el proceso de detección, utilizando un conjunto de métricas comunes.

A continuación, se presenta un cuadro comparativo entre el sistema actual (pre-test) y el modelo XGBoost (post-test) evaluando ambos en relación con sus respectivos entornos operativos.

Tabla 16

Métricas del pre-test y post-test

Indicador	Pre-test (Sistema Actual)	Post-test (Modelo XGBoost)
Enfoque	Automatizado basado en reglas	Modelo supervisado XGBoost
Precision	60%	84%
Recall	62%	73%
F1-Score	61%	78%
AUC	-	88%

Nota. Los valores del pretest fueron proporcionados internamente por el área de monitoreo actual. Los valores del postest corresponden a la ejecución del modelo XGBoost sobre los datos simulados (AMLSim).

5.2 DISCUSIÓN DE LOS RESULTADOS

5.2.1 Resultados descriptivos

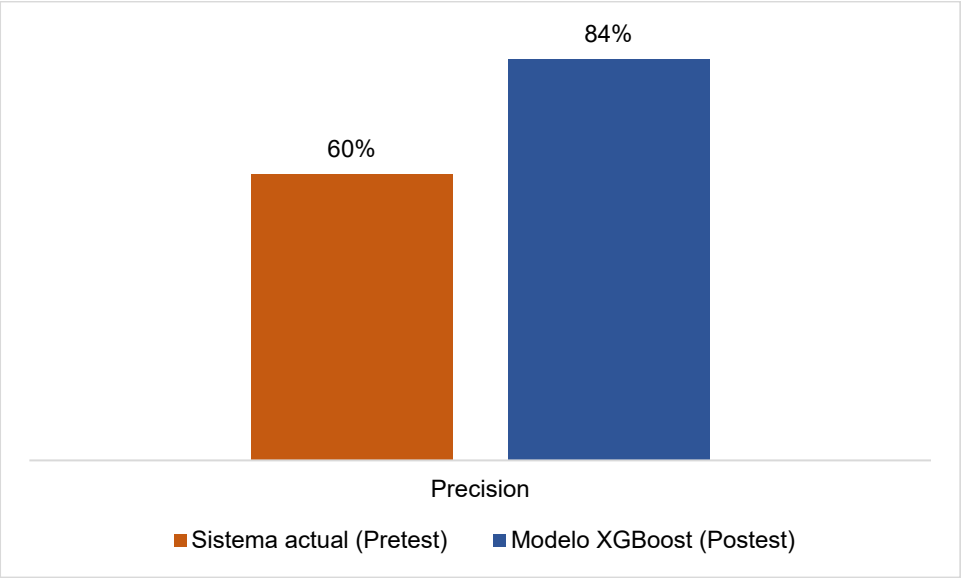
El presente apartado expone el análisis de las métricas de desempeño del modelo XGBoost en comparación con el sistema actual basado en reglas. Se evaluaron los indicadores clave de clasificación binaria: precisión, recall, F1-Score y AUC, los cuales permiten determinar la efectividad del modelo en la detección temprana de transacciones de lavado de activos. La comparación se realizó sobre una base de datos simulada proporcionada por el entorno AMLSim.

a) **Precisión (Precision):** Como se observa en la figura 39, la precisión alcanzada por el sistema actual fue de 60%, mientras que el modelo XGBoost logró un 84%, lo que representa una mejora de 24 puntos porcentuales. La precisión indica la proporción de transacciones clasificadas como sospechosas que realmente lo son. En el contexto de detección de lavado de activos, este incremento se traduce en una reducción significativa de falsos positivos, es decir, menos transacciones legítimas son marcadas erróneamente como sospechosas.

   Una mayor precisión reduce la carga de trabajo del personal de monitoreo, ya que disminuye la cantidad de alertas falsas que deben ser investigadas manualmente. Esto permite enfocar los recursos de cumplimiento en casos realmente críticos, mejorando la eficiencia del proceso y evitando la saturación del sistema de alertas.

Figura 39

Métrica Precision pre-test vs post-test



Nota. AMLSim-IBM

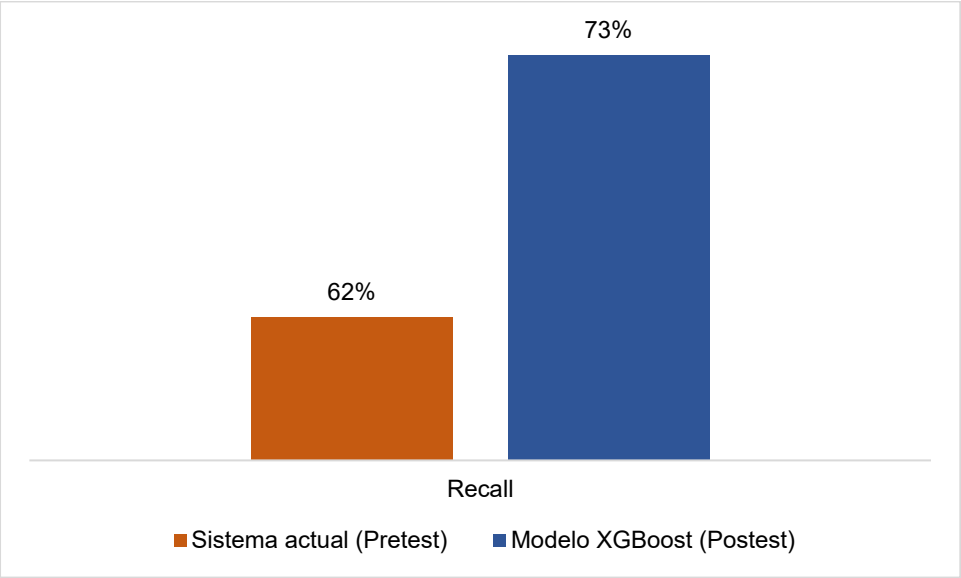
Elaboración propia

b) **Sensibilidad (Recall):** Como se observa en la figura 40, el sistema actual tuvo un recall de 62%, mientras que el modelo XGBoost obtuvo 73%, incrementando en 11 puntos porcentuales su capacidad para detectar transacciones realmente sospechosas. El recall mide la proporción de operaciones sospechosas que el modelo logra identificar correctamente. Un mayor recall significa que el modelo es capaz de detectar más casos verdaderamente sospechosos, lo cual es esencial en contextos financieros donde los falsos negativos pueden representar graves riesgos legales, regulatorios y reputacionales.

Esta mejora se traduce en una mayor cobertura de eventos críticos, permitiendo a la entidad anticiparse a esquemas complejos de lavado de dinero. Minimiza el riesgo de omitir transacciones de alto impacto y refuerza el cumplimiento normativo ante entidades reguladoras.

Figura 40

Métrica Recall pre-test vs post-test



Nota. AMLSim-IBM

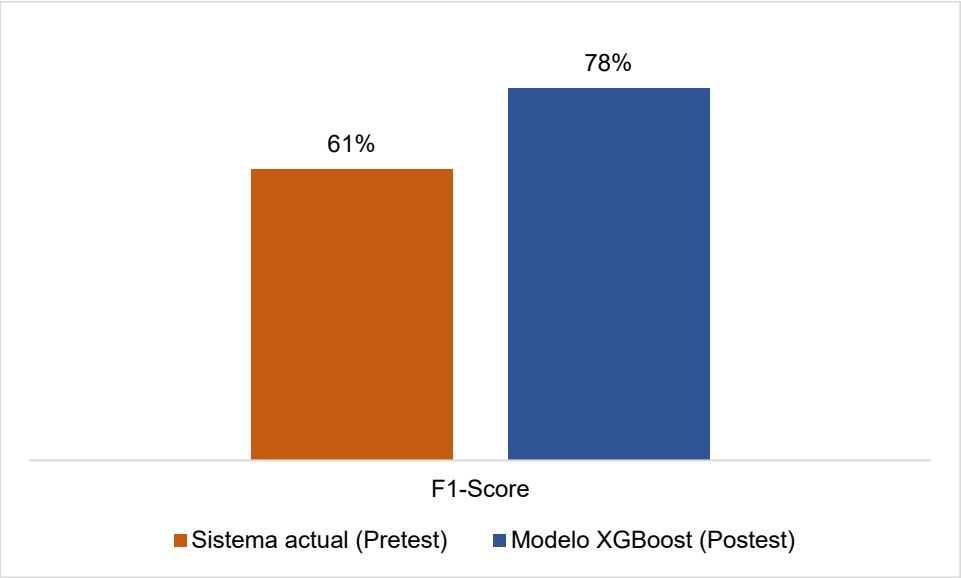
Elaboración propia

c) **F1-Score:** Como se observa en la figura 41, el F1-Score del sistema actual fue de 61%, mientras que el modelo XGBoost logró un 78%, mejorando en 17 puntos porcentuales. Esta métrica combina armónicamente la precisión y el recall, siendo especialmente útil cuando se busca un equilibrio entre la detección de transacciones sospechosas y la reducción de falsos positivos.

Un F1-Score elevado sugiere que el modelo no solo es preciso, sino también consistente en su rendimiento, lo que permite mantener un equilibrio robusto entre la eficacia del sistema y la eficiencia operativa. Esto garantiza decisiones más confiables en la gestión de alertas.

Figura 41

Métrica F1-Score pre-test vs post-test



Nota. AMLSim-IBM

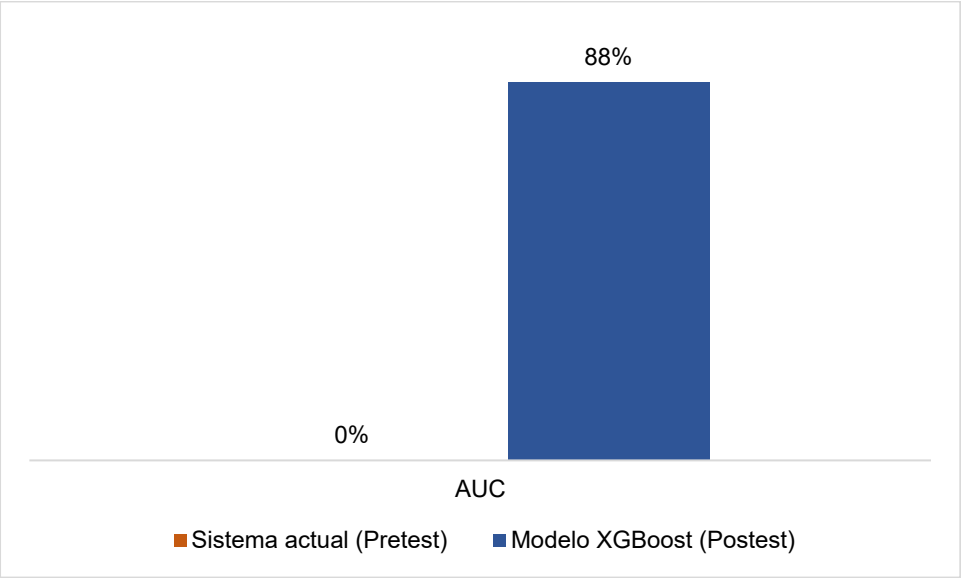
Elaboración propia

d) **Área bajo la curva ROC (AUC-ROC):** Como se observa en la figura 42, el sistema actual no presenta este indicador debido a su lógica determinista basada en reglas. Sin embargo, el modelo XGBoost obtuvo un AUC de 88%, lo que indica un alto nivel de capacidad para diferenciar entre transacciones sospechosas y no sospechosas.

Un AUC cercano al 90% evidencia que el modelo puede asignar puntajes de riesgo más precisos, facilitando la priorización de investigaciones en tiempo real. Esto favorece una gestión inteligente del riesgo operacional y permite enfocar recursos en transacciones con mayor probabilidad de fraude.

Figura 42

Métrica AUC-ROC pre-test vs post-test



Nota. AMLSim-IBM

Elaboración propia

5.2.2 Resultados inferenciales

El objetivo de este capítulo es contrastar la hipótesis general y las hipótesis específicas de la investigación, a través del análisis inferencial de las métricas de desempeño obtenidas en dos condiciones: el sistema actual (pre-test) y el modelo predictivo XGBoost (post-test). Se utilizó **la prueba t de Student para muestras independientes con varianzas desiguales (Welch's t-test)** para determinar si las diferencias observadas son estadísticamente significativas. Asimismo, se incluyeron gráficos de apoyo para una mejor interpretación de los resultados.

a) Grupos comparados

- **Pre-test:** Métricas proporcionadas por el sistema actual basado en reglas.
- **Post-test:** Métricas obtenidas por el modelo XGBoost

Se evaluaron tres métricas principales: Precisión, Recall (sensibilidad) y F1-Score. Cada métrica fue medida cinco veces en cada grupo.

Tabla 17

Métricas de la muestra de pre-test vs post-test

Métrica	Pre-test (n=5)	Post-test (n=5)
Precisión	0.58, 0.60, 0.59, 0.61, 0.60	0.83, 0.84, 0.85, 0.84, 0.83
Recall	0.60, 0.61, 0.62, 0.63, 0.62	0.72, 0.73, 0.74, 0.73, 0.74
F1-Score	0.59, 0.60, 0.61, 0.62, 0.61	0.77, 0.78, 0.79, 0.78, 0.77

Nota. Los valores del pretest fueron proporcionados internamente por el área de monitoreo actual. Los valores del postest corresponden a la ejecución del modelo XGBoost sobre los datos simulados (AMLSim).

b) **Nivel se significancia:** Se estableció un nivel de significancia de $\alpha = 0.05$. Esto significa que si el p-valor obtenido en la prueba t es menor que 0.05, se considera que hay una diferencia estadísticamente significativa entre los grupos. Además, esto significa que se acepta un margen de error del 5% al momento de rechazar la hipótesis nula.

c) **Fórmulas empleadas:** Para contrastar las hipótesis específicas, se aplicó la prueba t de Student para muestras independientes con varianzas desiguales, también conocida como prueba t de Welch. Esta prueba se utiliza cuando se desea comparar dos grupos diferentes, como es el caso de esta investigación).

   Según Ruxton (2006), la prueba t de Welch es más robusta que la prueba t clásica cuando los tamaños de muestra son pequeños y las varianzas son distintas, como ocurre en este estudio.

   El valor del estadístico t se calcula con la siguiente Ecuación 13:

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{\frac{{s_1}^2}{n_1} + \frac{{s_2}^2}{n_2}}} \qquad (13)$$

   Donde:

   - $\overline{X_1}$: media de la métrica en el grupo post-test

- $\overline{X_2}$: media de la métrica en el grupo pre-test
- ${s_1}^2$, ${s_2}^2$: varianzas muestrales de cada grupo
- n_1, n_2: tamaños de la muestra

Este estadístico permite evaluar qué tan grande es la diferencia entre medias, en relación con la variabilidad de los datos.

El número de grados de libertad se estima mediante la Ecuación 14 de Welch-Satterthwaite, la cual ajusta los grados de libertad cuando las varianzas y tamaños de muestra son diferentes (Welch, 1947; Satterthwaite, 1946):

$$df = \frac{(\frac{{s_1}^2}{n_1} + \frac{{s_2}^2}{n_2})}{\frac{(\frac{{s_1}^2}{n_1})^2}{n_1 - 1} + \frac{(\frac{{s_2}^2}{n_2})^2}{n_2 - 1}} \qquad (14)$$

El p-valor es calculado a partir del estadístico t y el valor df.

d) Resultados de la prueba t de Welch

Ahora presentamos en la Tabla 18 los resultados de cada métrica para los grupos de pre-test y post-test:

Tabla 18

Resultados de la prueba t de Welch para la comparación de métricas entre el sistema actual y el modelo XGBoost

Métrica	Media Pre-test	Media Post-test	t-valor	p-valor	Significativo
Precisión	0.596	0.838	38.264	<0.001	Sí
Recall	0.616	0.732	18.341	<0.001	Sí
F1-Score	0.606	0.778	27.196	<0.001	Sí

Nota. Elaboración propia

e) **Contrastación de hipótesis:** En esta sección se contrastan las hipótesis específicas, con base en los resultados inferenciales obtenidos mediante la prueba t de Student para muestras independientes con varianzas desiguales (Welch's t-test). Se utilizó un nivel de significancia de $\alpha = 0.05$. A continuación, se detalla el análisis para cada hipótesis.

Prueba de Hipótesis Específica 1 (HE1)

Planteamiento

- **Hipótesis nula (H_0):** La implementación del modelo predictivo seleccionado no influye significativamente en el incremento de la sensibilidad (Recall) en la detección temprana de transacciones de lavado de activos en entidades financieras.
- **Hipótesis alternativa (H_1):** La implementación del modelo predictivo seleccionado influye significativamente en el incremento de la sensibilidad (Recall) en la detección temprana de transacciones de lavado de activos en entidades financieras.

Evidencia:

- Pre-test: promedio de recall=0.616
- Post-test: promedio de recall=0.732
- t-valor=18.341
- p-valor= 0.001
- Nivel de significancia (α)= 0.05

Criterio de decisión:

Según la teoría inferencial (Field, 2013; Montgomery, 2017):

- Si p-valor < α(0.005) → Se rechaza la hipótesis nula (H_0) y se acepta la hipótesis alternativa (H_1)
- Si p-valor > α(0.005) → No se rechaza la hipótesis nula (H_0)

Análisis:

Dado que:

- p-valor = 0.001<0.005

Entonces, se rechaza H_0 y se concluye que existe una diferencia estadísticamente significativa en el recall entre el pre-test y post-test. Esto implica que la implementación del modelo predictivo influye positivamente en la mejora de la sensibilidad (recall) para detectar transacciones de lavado de activos en entidades financieras.

Conclusión formal:

A un nivel de significancia del 5%, los resultados indican evidencia estadísticamente significativa **para rechazar la hipótesis nula y aceptar la hipótesis alternativa HE1**, validando que la implementación del modelo predictivo seleccionado, XGBoost, mejora significativamente el recall en la detección de lavado de activos en entidades financieras. Esto implica menos falsos negativos, es decir, menos casos que pasan desapercibidos. En el contexto de cumplimiento normativo, esta mejora reduce el riesgo de omitir transacciones de lavado de activos sospechosas, lo que es clave para evitar sanciones legales o regulatorias.

Prueba de Hipótesis Específica 2 (HE2)

Planteamiento

- **Hipótesis nula (H_0):** La implementación del modelo predictivo seleccionado no influye significativamente en el incremento de la precisión (Precision) en la detección temprana de transacciones de lavado de activos en entidades financieras.
- **Hipótesis alternativa (H_1):** La implementación del modelo predictivo seleccionado influye significativamente en el incremento de la precisión (Precision) en la detección temprana de transacciones de lavado de activos en entidades financieras.

Evidencia:

- Pre-test: promedio de la precisión=0. 596
- Post-test: promedio de la precisión=0. 838
- t-valor= 38.264

- p-valor= 0.001
- Nivel de significancia (α)= 0.05

Criterio de decisión:

Según la teoría inferencial (Field, 2013; Montgomery, 2017):

- Si p-valor < α(0.005) → Se rechaza la hipótesis nula ($\boldsymbol{H_0}$) y se acepta la hipótesis alternativa ($\boldsymbol{H_1}$)
- Si p-valor > α(0.005) → No se rechaza la hipótesis nula ($\boldsymbol{H_0}$)

Análisis:

Dado que:

- p-valor = 0.001<0.005

Entonces, se rechaza H_0 y se concluye que existe una diferencia estadísticamente significativa en la precisión entre el pre-test y post-test. Esto implica que la implementación del modelo predictivo influye positivamente en la mejora de la sensibilidad (recall) para detectar transacciones de lavado de activos en entidades financieras.

Conclusión formal:

A un nivel de significancia del 5%, los resultados indican evidencia estadísticamente significativa **para rechazar la hipótesis nula y aceptar la hipótesis alternativa HE2**, validando que la implementación del modelo predictivo seleccionado, XGBoost, mejora significativamente la precisión en la detección de lavado de activos en entidades financieras. Esto se traduce en una menor carga de trabajo para los analistas de cumplimiento, ya que hay menos alertas falsas que revisar. Mejora la eficiencia del área y reduce los costos operativos asociados a la validación manual de transacciones.

Prueba de Hipótesis Específica 3 (HE3)

Planteamiento

- **Hipótesis nula ($\boldsymbol{H_0}$):** La implementación del modelo predictivo seleccionado no influye significativamente en el incremento del

área bajo la curva ROC (AUC-ROC) en la detección temprana de transacciones de lavado de activos en entidades financieras.

- **Hipótesis alternativa (H_1):** La implementación del modelo predictivo seleccionado influye significativamente en el incremento del área bajo la curva ROC (AUC-ROC) en la detección temprana de transacciones de lavado de activos en entidades financieras.

Evidencia:

- Pre-test: No aplicable (el sistema basado en reglas no genera puntuaciones de probabilidad, por lo que no permite calcular el AUC-ROC).
- Post-test: AUC=0.88
- Nivel de significancia (α)= 0.05

Análisis:

Dado que el sistema actual opera bajo un esquema de reglas fijas, no es posible calcular el AUC-ROC para el pretest, ya que esta métrica requiere una salida continua de probabilidades para distintos umbrales de clasificación. Sin embargo, al aplicar el modelo XGBoost, que si entrega probabilidades de predicción, se obtiene un valor de AUC de 0.88, lo cual representa un excelente nivel de discriminación entre clases (transacciones sospechosas y no sospechosas).

Conclusión formal:

A un nivel de significancia del 5%, los resultados del post-test evidencian que el modelo XGBoost presenta un AUC-ROC elevado, lo que indica una alta capacidad de discriminación en la detección de transacciones de lavado de activos. Aunque no fue posible calcular el AUC en el sistema actual, los resultados obtenidos con el modelo propuesto **sustentan la aceptación de la hipótesis específica HE3**, en tanto se demuestra una mejora cualitativa significativa respecto a la capacidad de clasificación del sistema. Esto se traduce con contar con un modelo que calcula probabilidades que permite:

- Establecer umbrales de alerta personalizadas
- Automatizar la priorización de transacciones sospechosas

En conclusión, los resultados estadísticos obtenidos a través de las pruebas de hipótesis específicas HE1, HE2 y HE3 evidencian de manera consistente que la implementación del modelo predictivo XGBoost mejora significativamente el desempeño en la detección temprana de transacciones de lavado de activos en entidades financieras.

En detalle, se observaron mejoras estadísticamente significativas tanto en la sensibilidad (recall), como en la precisión (precision), con p-valores inferiores al nivel de significancia del 5%, lo cual permite rechazar las hipótesis nulas correspondientes y aceptar que el modelo influye positivamente en ambas métricas. Asimismo, aunque no se pudo realizar una comparación directa del AUC-ROC con el sistema previo basado en reglas, el valor alcanzado por el modelo (0.88) representa una alta capacidad de discriminación, lo cual aporta evidencia cualitativa solida a favor de su efectividad.

En conjunto, estos hallazgos validan empíricamente que el modelo XGBoost no solo mejora la capacidad de identificar correctamente las transacciones sospechosas (recall), sino que también reduce los falsos positivos (precisión), optimizando así los recursos de monitoreo. Además, su capacidad para generar probabilidades permite establecer umbrales flexibles y priorizar alertas, superando las limitaciones del sistema actual.

Esta mejora integral en el rendimiento del sistema de detección representa un avance significativo en términos de cumplimiento normativo, eficiencia operativa y prevención de riesgos reputacionales y legales.

CONCLUSIONES

- La implementación de un modelo predictivo de aprendizaje automático, en particular XGBoost, mejora en la detección temprana de transacciones sospechosas de lavado de activos en entidades financieras. El modelo demostró un desempeño sólido en las métricas clave evaluadas, consolidándose como una herramienta eficaz para fortalecer los sistemas de prevención en el sector financiero.

- La implementación del modelo XGBoost permitió alcanzar una sensibilidad (recall) del 73%, lo que demuestra su capacidad para identificar correctamente una proporción considerable de transacciones sospechosas de lavado de activos. Este resultado resalta la eficacia del modelo en la detección de casos positivos, reduciendo el riesgo de falsos negativos y contribuyendo significativamente al fortalecimiento de los mecanismos de prevención en las entidades financieras.

- En relación con la precisión (Precision), el modelo predictivo seleccionado alcanzó un valor del 84%, lo que implica que la mayoría de las transacciones identificadas como sospechosas realmente lo son. Esto es fundamental para reducir el número de falsos positivos, lo cual optimiza los recursos destinados a la investigación de actividades de lavado de activos, incrementando la eficiencia del sistema de detección.

- El área bajo la curva ROC (AUC-ROC) alcanzada por el modelo XGBoost fue de 88%, lo que refleja una elevada capacidad discriminativa para diferencias entre transacciones sospechosas y no sospechosas. Este nivel de desempeño reafirma la efectividad del modelo en la clasificación binaria dentro del contexto del lavado de activos, contribuyendo a una detección más precisa y confiable en escenarios reales.

- El análisis inferencial confirmó mejoras estadísticamente significativas en las métricas de desempeño (precision, recall, AUC-ROC) tras implementar el modelo XGBoost, respaldando la hipótesis general de que este modelo mejora la detección temprana de transacciones de lavado de activos.

RECOMENDACIONES

- Se recomienda adoptar el modelo XGBoost en las plataformas de monitoreo de transacciones de las entidades financieras, debido a su balance entre precisión y capacidad de detección de casos positivos. Su alto desempeño en métricas como Recall (73%) y AUC-ROC (88%) lo posiciona como una herramienta robusta para la identificación temprana de operaciones sospechosas.

- Aunque esta investigación no abordó el despliegue y monitoreo, se sugiere que, en un entorno productivo, se incluya un componente de vigilancia de desempeño basado en MLOps. Esto permitirá detectar el drift de datos y realizar ajustes periódicos para mantener la precisión del modelo ante posibles cambios en los patrones de transacciones.

- Se recomienda incorporar variables exógenas adicionales como historial crediticio, actividad geográfica o comportamiento en plataformas digitales. Estas variables pueden enriquecer la representación de las operaciones financieras y aumentar el poder predictivo de los modelos.

- La validación futura del modelo podría realizarse en entornos con datos reales o en un *sandbox* regulatorio, lo cual permitiría confirmar la efectividad del modelo en escenarios reales y ajustar sus parámetros con mayor precisión.

REFERENCIAS BIBLIOGRÁFICAS

Agresti, A. (2018). *Statistical Methods for the Social Sciences* (5a ed.). Pearson Educación.

Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review, 40*, 100402. https://doi.org/10.1016/j.cosrev.2021.100402

Alpaydin, E. (2010*). Introduction to Machine Learning* (2a Ed.). Massachusetts Institute of Technology.

Alvear, J. E. L., & Micheli, E. L. (2019). La anterior actividad ilícita de lavado de dinero en el Sistema jurídico ecuatoriano (año de referencia 2014). *Revista Facultad de Jurisprudencia*, (5), 1-15. https://www.redalyc.org/articulo.oa?id=600263495005

Bahamón-Jara, M. L., Cujabante-Villamil, X. A., & Durán-Montaño, A. C. (2021). Lavado de dinero y corrupción: necesidad de mayor investigación para un sustento empírico sólido. Via Inveniendi Et Iudicandi, 16(2). https://doi.org/10.15332/19090528.6781

Banco Mundial. (2019). Combatting money laundering and terrorist financing: A model of good practices for financial institutions.

Barbosa-Moreno, A., Mar-Orozco, C., Molar-Orozco, J. (2020). *Metodología de la investigación. Métodos y técnicas*. Grupo Editorial Patria

Bergstra, J., & Bengio, Y. (2012). Random search for hyper-parameter optimization*. Journal of Machine Learning Research, 13*, 281–305.

Berrendorf, M. (2022). Machine learning for managing structured and semi-structured data [Tesis de maestría, LMU München]. Elektronische Hochschulschriften. https://edoc.ub.uni-muenchen.de/29401/

Biau, G., & Scornet, E. (2016). A random forest guided tour. *TEST, 25*(2), 197–227. https://doi.org/10.1007/s11749-016-0481-7

Bishop, C. M. (1995*). Neural networks for pattern recognition*. Oxford university press.

Bishop, C.M. (2006). *Pattern Recognition and Machine Learning*. Springer.

Blanco-Cordero, I., Fabián-Caparrós, E., Prado-Saldarriaga, V., Santander-Abril, G., y Zaragoza-Aguado, J. (2014). *Combate al Lavado de Activos desde el Sistema Judicial* (5a ed.). Organización de los Estados Americanos – OEA

Bravo-Acevedo, G. (2021). Seguridad, migración, trata de personas y tráfico de migrantes en Chile (2010-2018). *Revista De Historia Americana Y Argentina*, 56(2), 209–231. https://doi.org/10.48162/rev.44.017

Breiman, L. (2001). Random forests. *Machine Learning*, 45(1), 5–32. https://doi.org/10.1023/A:1010933404324

Brownlee, J. (2019). *XGBoost With Python*. Machine Learning Mastery.

Burges, C. J. (1998). A Tutorial on Support Vector Machines for Pattern Recognition. *Data Mining and Knowledge Discovery, 2*, 121–167. https://doi.org/10.1023/A:1009715923555

Burgos, C., & Manterola, C. (2010). Cómo interpretar un artículo sobre pruebas diagnósticas. *Revista Chilena de Cirugía*, 62(62), 301-308. https://doi.org/10.4067/S0718-40262010000300018

Cánovas, F., Alonso, F., Gomariz, F. & Oñate, F. (2017). Modification of the random forest algorithm to avoid statistical dependence problems when classifying remote sensing imagery. *Computers & Geosciences*, 103, 1-11. https://doi.org/10.1016/j.cageo.2017.02.012.

Castillo Ramos, M. E., & Muriel Páez, M. (2023). La trata de seres humanos para explotación criminal y el principio de no punibilidad de las víctimas. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, 4(2), 1866–1875. https://doi.org/10.56712/latam.v4i2.709

Chapelle, O. (2010). *Aprendizaje automático: un enfoque práctico*. MIT Press.

Chapelle, O., Scholk. B., & Zien, A. (2006). *Semi-Supervised Learning*. MIT Press.

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic Minority Over-sampling Technique. *Journal of Artificial Intelligence Research,* 16, 321-357. https://doi.org/10.1613/jair.953

Chen, T. & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data*, 785-794. KDD '16. https://doi.org/10.1145/2939672.2939785.

Chen, Z., Van Khoa, L. D., Teoh, E. N., Nazir, A., Karuppiah, E. K., & Lam, K. S. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: *A review. Knowledge and Information Systems*, 57, 245-285. https://doi.org/10.1007/s10115-017-1144-z

Correa Bahnsen, A., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications*, *51*, 134–142. https://doi.org/10.1016/j.eswa.2015.12.030

Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning, 20*, 273–297. https://doi.org/10.1007 /bf00994018

Cortés-Sánchez, J. S. (2023). Detección de anomalías Transaccionales Aplicando Técnicas de Machine Learning con Grafos [Tesis de grado, Universidad del Rosario]. Repositorio Institucional E-docUR. https://repository.urosario.edu.co/handle/10336/40983

Cover, T., & Hart, P. (1967). Nearest neighbor pattern classification. *IEEE Transactions on Information Theory, 13*(1), 21–27. https://doi.org/10.1109/TIT.1967.1053964

Cuellar, G. G. (2018). Lavado de activos: organización y particularidades. Revista Pensamiento Penal.

De Cunto, A. L. (2021). La antijuridicidad y la responsabilidad por acto lícito. *Dossier doctrinario. Autores de Chubut, 82*, 324. http://www.derecho.uba.ar/publicaciones/

Delamaire, L., Abdou, H., & Pointon, J. (2009). Credit card fraud and detection techniques: A review. *Banks and Bank Systems*, *4*(2), 57–68.

Espinosa-Zúñiga, J. J. (2020). Aplicación de algoritmos Random Forest y XGBoost en una base de solicitudes de tarjetas de crédito*. Ingeniería Investigación Y Tecnología, 21(3)*, 1–16. https://doi.org/10.22201/fi.25940732e.2020.21.3.022

Ezcurra-Silva, A. R. (2016). Desarrollo de una metodología de identificación y evaluación de riesgos de lavado de activos y financiamiento al terrorismo en una sociedad titulizadora [Tesis de grado, Universidad Nacional de Ingeniería]. Repositorio Institucional. http://hdl.handle.net/20.500.14076/5388

Fawcett, T. (2006). An introduction to ROC analysis. *Pattern Recognition Letters*, 27(8), 861-874.

Fernández-Murillo, J., Bravo-Rosillo, G., Zambrano-Zambrano, E. (2022). Lavado de activos y su efecto en las inversiones del sector empresarial en el Ecuador. ECA Sinergia, 13(2), 118-128 Universidad Técnica de Manabí Ecuador DOI: https://doi.org/10.33936/eca_sinergia.v13i1

Field, A., Miles, J., & Field, Z. (2012). *Discovering statistics using R* (1a ed.). Sage Publications Ltd.

Foley, S., Karlsen, J. R., & Putniii, T. J. (2018). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *Review of Financial Studies, Forthcoming*, 63. https://doi.org/10.2139/ssrn.3102645

Fondo Monetario Internacional. (2018). *Hablando claro: Lavado de dinero*. Finanzas & Desarrollo. https://www.imf.org/external/pubs/ft/fandd/spa/2018/12/pdf/straight.pdf

Friedman, J., Hastie, T., & Tibshirani, R. (2009). *The Elements of Statistical Learning: Data Mining, Inference, and Prediction* (2nd ed.). Springer. https://doi.org/10.1007/978-0-387-84858-7

GAFILAT (2017*). Informe de amenazas regionales en materia de lavado de activos.* Grupo de Acción Financiera de Latinoamérica.

GAFI. (2020). *The FATF Recommendations*. Financial Action Task Force.

Galeano-Villar, A. J., & Vargas-Cisneros, Z. N. (2019). Modelos de aprendizaje automático aplicados a la detección de transacciones sospechosas de lavado de activos en entidades financieras: Una revisión sistemática de la literatura [Tesis de grado, Universidad Peruana Unión]. Repositorio de Tesis. http://hdl.handle.net/20.500.12840/2519

García, S., Sánchez, J. S., & Mollineda, R. A. (2009). An overview of outlier detection methodologies. *Pattern Recognition*, 40(12), 3447-3460. https://doi.org/10.1016/j.patcog.2009.03.009

Géron, A. (2019). *Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow: Concepts, tools, and techniques to build intelligent systems* (2nd ed.). O'Reilly Media.

Ghulam, Y., & Szalay, B. (2024). Investigating the determinants of money laundering risk. *Journal of Money Laundering Control*, 27(1), 139-157. https://doi.org/10.1108/JMLC-01-2023-0001.

Glorot, X., Bordes, A., & Bengio, Y. (2011). Deep sparse rectifier neural networks. *Proceedings of the Fourteenth International Conference on Artificial Intelligence and Statistics*, *15*, 315–323. https://proceedings.mlr.press/v15/glorot11a.html

González-Revaldería, J., Fernández, J. M. P., García, B. P., & Queraltó, J. M. (2007). *Curso de estadística para el laboratorio clínico. módulo 3: Regresión logística*. Sociedad Española de Bioquímica Clínica y Patología Molecular.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

Gracia Granados, M. (2016). Detección de operaciones sospechosas de lavado de activos en el sistema financiero, usando variables no transaccionales, máquinas de soporte vectorial y árboles de clasificación. *Universidad de Antioquia*. http://hdl.handle.net/10495/13736

Han, J., Kamber, M., & Pei, J. (2012). *Data mining: concepts and techniques* (3rd ed.). Morgan Kaufmann.

Hassan, M., Aziz, L. A.-R., & Andriansyah, Y. (2023). The Role Artificial Intelligence in Modern Banking: An Exploration of AI-Driven

Approaches for Enhanced Fraud Prevention, Risk Management, and Regulatory Compliance. *Reviews of Contemporary Business Analytics*, 6(1), 110–132. https://researchberg.com/index.php/rcba/article/view/153

Hastie, T., Tibshirani, R., & Friedman, J. H. (2009). *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. Springer Series in Statistics.

Haykin, S. (1999). *Neural networks. A comprehensive foundation*. Prentice Hall International Inc.

Haykin, S. S. (2009). *Neural Networks and Learning Machines*. Pearson Educación.

Hosmer, D. W., Lemeshow, S., & Sturdivant, R. X. (2013). *Applied Logistic Regression* (3a ed.). John Wiley & Sons, Hoboken, NJ. https://doi.org/10.1002/9781118548387

Hsu, C.-W., Chang, C.-C., & Lin, C.-J. (2003). *A practical guide to support vector classification* (Tech. Rep. No. 2003). Department of Computer Science, National Taiwan University. https://www.csie.ntu.edu.tw/~cjlin/papers/guide/guide.pdf

Kaelbling, L. P., Littman, M. L., & Moore, A. W. (1996). Reinforcement learning: A survey. *Journal of artificial intelligence research*, 4, 237-285. https://doi.org/10.1613/jair.301

Kaur, S. (2019). Money Laundering a Fast Growing Menace: Emerging Trends and Measures to Curb. *International Journal of Research in Social Sciences,* 9(6), 247-262. https://www.indianjournals.com/ijor.aspx?target=ijor:ijrss&volume=9&issue=6&article=020

Kingma, D. P., & Ba, J. (2015). Adam: A method for stochastic optimization. *In 3rd International Conference on Learning Representations (ICLR)*, San Diego, USA. arXiv. https://doi.org/10.48550/arXiv.1412.6980

Kish, L. (1965). *Survey sampling*. John Wiley & Sons.

Kohavi, R. (1995). A study of cross-validation and bootstrap for accuracy estimation and model selection. *Proceedings of the 14th International Joint Conference on Artificial Intelligence (IJCAI)*, 1137-1145.

Kreuzberger, D., Kühl, N., & Hirschl, S. (2022). *Machine Learning Operations (MLOps): Overview, definition, and architecture*. arXiv. https://doi.org/10.48550/arXiv.2205.02302, D., Kühl, N., & Hirschl, S. (2022). *Machine Learning Operations (MLOps): Overview, definition, and architecture*. arXiv. https://doi.org/10.48550/arXiv.2205.02302

Kuha, J., & Mills, C. (2020). On group comparisons with logistic regression models. *Sociological Methods & Research*, 49(2), 498-525. https://doi.org/10.1177/00491241177473

Kumar, P. (2015). Money Laundering in India: Concepts, Effects and Legislation. *International Journal of Research*, 3(7), 51-63. https://www.raijmr.com/ijrhs/wp-content/uploads/2017/11/IJRHS_2015_vol03_issue_07_11.pdf

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444. https://doi.org/10.1038/nature14539

Liaw, A., & Wiener, M. (2002). Classification and regression by randomForest. *R news*, 2(3), 18-22. https://journal.r-project.org/articles/RN-2002-022/RN-2002-022.pdf

Lizares, M. (2017). Comparación de modelos de clasificación: regresión logística y árboles de clasificación para evaluar el rendimiento académico [Tesis de pregrado, Universidad Nacional Mayor de San Marcos]. Repositorio institucional Cybertesis UNMSM. https://hdl.handle.net/20.500.12672/7122

Loh, W.-Y. (2011). *Classification and regression trees*. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 1(1), 14–23. https://doi.org/10.1002/widm.8

Lokanan, M. E. (2024). Predicting money laundering using machine learning and artificial neural networks algorithms in banks. *Journal of Applied Security Research,* 19(1), 20-44. https://doi.org/10.1080/19361610.2022.2114744

Loría, E., & Salas, E. (2019). La relación entre robo y desempleo de varones jóvenes en México, 2005-2017. *Revista mexicana de economía y finanzas*, 14(3), 433-446. https://doi.org/10.21919/remef.v14i3.353

Lucero-Chunir, M. M., & Sánchez-Gutiérrez, J. A. (2023). Implicancias penales del lavado de activos en Ecuador. *MQRInvestigar*, 7(1), 1382–1406. https://doi.org/10.56048/MQR20225.7.1.2023.1382-1406

Luna-Galván, M., Luong, H. T., & Astolfi, E. (2021). El narcotráfico como crimen organizado: comprendiendo el fenómeno desde la perspectiva trasnacional y multidimensional. *Revista de Relaciones Internacionales, Estrategia y Seguridad*, 16(1), 197-212. https://doi.org/10.18359/ries.5412

Maiola, O. (2015). El Fraude y la corrupción subyacentes en los Estados Contables: complemento de la matriz de riesgos descontada, su valor actual neto y medidas de tendencia central en encuestas sobre delitos contables y empresariales. *Contabilidad Y Auditoría*, (40), 34. https://ojs.econ.uba.ar/index.php/Contyaudit/article/view/751

Manrique-Rojas, E. (2020). Machine Learning: análisis de lenguajes de programación y herramientas para desarrollo. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (E28), 586-599. https://www.proquest.com/docview/2388304894?pq-origsite=gscholar&fromopenview=true&sourcetype=Scholarly%20Journals

Martínez-Camblor, P. (2007). Comparación de pruebas diagnósticas desde la curva ROC. *Revista Colombiana de Estadística*, 30(2), 163-176. https://revistas.unal.edu.co/index.php/estad/article/view/29454

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955. *AI magazine*, 27(4), 12-12. https://doi.org/10.1609/aimag.v27i4.1904

Mitchell, T. (1997). *Machine Learning*. McGraw-Hill Interamericana.

Molina-Salvador, R. F. (2016). Análisis de cluster de K-medias y técnica Chaid para la segmentación y clasificación de personas naturales en el

mercado bursátil limeño para la prevención de lavado de activos [Tesis de grado, Universidad Nacional de Ingeniería]. Repositorio Institucional. http://hdl.handle.net/20.500.14076/4948

Murphy, K. P. (2012). *Machine Learning A Probabilistic Perspective*. Massachusetts Institute of Technology.

Nayyer, N., Javaid, N., Akbar, M., Aldegheishem, A., Alrajeh, N., & Jamil, M. (2023). A New Framework for Fraud Detection in Bitcoin Transactions Through Ensemble Stacking Model in Smart Cities. *IEEE Access, 11,* 90916-90938. https://doi.org/10.1109/ACCESS.2023.3308298.

Němec, S. (2019). *Machine learning for financial crime detection.* Faculty Of Information Technology CTU In Prague. Czech Technical University.

Ng, A. Y. (2004). Feature selection, L1 vs. L2 regularization, and rotational invariance. *Proceedings of the 21st International Conference on Machine Learning (ICML '04)*, 78. Association for Computing Machinery. https://doi.org/10.1145/1015330.1015435

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Nielsen, D. (2016). Tree Boosting With XGBoost - Why Does XGBoost Win "Every" Machine Learning Competition? NTNU, Norwegian University of Science and Technology.

Norvig, P. (2012). Artificial intelligence: Early ambitions. NewScientist, 216(2889), ii-iii. https://doi.org/10.1016/S0262-4079(12)62783-3

Ocaña-Fernández, Y., Valenzuela-Fernández, L. A., & Garro-Aburto, L. L. (2019). Inteligencia artificial y sus implicaciones en la educación superior. *Propósitos y representaciones*, 7(2), 536-568. http://dx.doi.org/10.20511/pyr2019.v7n2.274

Ordoñez Bolaños, A. A., Rojas, J. S., Gómez Gómez, J., & Ramírez-González, G. (2023). Metodología basada en MLOps (Machine Learning Operations) para apoyo a la gestión en proyectos de ciencia de datos.

Revista Colombiana de Tecnologías de Avanzada (RCTA), *1*(41), 87–103. https://doi.org/10.24054/rcta.v1i41.2510

Palombini, V. V. (2021). Persecución penal del delito de lavado de activos [Tesis de grado, Universidad Nacional del Comahue]. Repositorio Digital Institucional. http://rdi.uncoma.edu.ar/handle/uncomaid/16523

Pearl, J. (1988). *Probabilistic reasoning in intelligent systems: Networks of plausible inference*. Morgan Kaufmann.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... & Duchesnay, É. (2011). Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12, 2825-2830.

Phua, C., Lee, V., Smith-Miles, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *CoRR*, *abs/1009.6119*. https://arxiv.org/abs/1009.6119

Ponce-Andrade, A. L., Piedrahita-Bustamante, P., & Villagómez-Cabezas, R. Í. (2019). Toma de decisiones y responsabilidad penal frente al lavado de activos en Ecuador. *Política Criminal*, 14(28), 365–384. https://doi.org/10.4067/s0718-33992019000200365

Powers, D. M. W. (2011). Evaluation: From precision, recall and F-measure to ROC, informedness, markedness & correlation. *Journal of Machine Learning Technologies*, *2*(1), 37–63. https://doi.org/10.9735/2229-3981

Probst, P., Wright, M., & Boulesteix, A.-L. (2019). *Hyperparameters and tuning strategies for random forest*. arXiv. https://doi.org/10.48550/arXiv.1804.03515

Qiu, Y., Zhou, J., Khandelwal, M., Yang, H., Yang, P., & Li, C. (2021). Performance evaluation of hybrid WOA-XGBoost, GWO-XGBoost and BO-XGBoost models to predict blast-induced ground vibration. *Engineering with Computers*, 1-18. https://doi.org/10.1007/s00366-021-01393-9

Quinlan, J. R. (1986). Induction of decision trees. *Machine Learning*, 1(1), 81-106.

Quintero-Acuña, L. K. (2023). Aplicación de Machine Learning a un modelo tradicional de Prevención y detección de fraude en entidad financiera

proyectados periodos trimestrales [Tesis de grado, Universidad la Salle]. *Ciencia Unisalle.* https://ciencia.lasalle.edu.co/maest_analitica_inteligencia_negocios/7/

Quishpe-Oña, J. B. (2022). Desarrollo e implementación de modelos de segmentación de clientes basados en machine learning para detectar riesgos de lavados de activos y financiación del terrorismo. Caso de estudio en una aseguradora [Tesis de maestría, Escuela Politécnica Nacional]. BIBDIGITAL. http://bibdigital.epn.edu.ec/handle/15000/23034

Ricardo, J. E., Vázquez, M. Y. L., Palacios, A. J. P., & Ojeda, Y. E. A. (2021). Inteligencia artificial y propiedad intelectual. *Universidad y Sociedad*, 13(S3), 362-368. https://rus.ucf.edu.cu/index.php/rus/article/view/2490.

Rich, E., & Knight, K. (1991). *Artificial Intelligence*. McGraw-Hill Interamericana.

Rodríguez-Mallma, J. R. (2022). Proyecto de implementación de un modelo Machine Learning para la evaluación de riesgo de operaciones sospechosas a los clientes de una entidad bancaria [Tesis de grado, Universidad Nacional Mayor de San Marcos]. CYBERTESIS. https://hdl.handle.net/20.500.12672/17960

Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). Learning internal representations by error propagation. *In Parallel distributed processing: explorations in the microstructure of cognition*. The MIT Press.

Russell, S. J., & Norvig, P. (2004). *Inteligencia artificial. Un enfoque moderno* (2a ed.). Pearson Educación.

Ruxton, G. D. (2006). The unequal variance t-test is an underused alternative to Student's t-test and the Mann–Whitney U test. *Behavioral Ecology*, 17(4), 688–690.

Ryman-Tubb, N., Krause, P., & Garn, W. (2018). How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence, 76*, 130–157. https://doi.org/10.1016/j.engappai.2018.07.008

Saavedra-Leyva, R. E., Morones-Carrillo, A. L., & Martínez-Sidón, G. (2021). El robo como obstáculo para el emprendimiento en México, 2005-2018. *Análisis económico, 36*(92), 145-163. https://doi.org/10.24275/uam/azc/dcsh/ae/2021v36n92/saavedra

Sagi, O., & Rokach, L. (2021). Approximating XGBoost with an interpretable decision tree. *Information Sciences*, 572, 522-542. https://doi.org/10.1016/j.ins.2021.05.055

Saito, T., & Rehmsmeier, M. (2015). The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets. *PLoS ONE, 10*(3), e0118432. https://doi.org/10.1371/journal.pone.0118432

Samuel, A. L. (1959). Some studies in machine learning using the game of checkers. *IBM Journal of research and development, 3*(3), 210-229. https://doi.org/10.1147/rd.33.0210

Santillán-Molina, A. L., Vinueza-Ochoa, N. V., Benavides-Salazar, C. F., & Santillán-Ojeda, S. J. (2022). Drogas, tráfico y crimen organizado como detonante de actos violentos en las cárceles del Ecuador. *Revista Universidad y Sociedad, 14*(3), 478-486. https://rus.ucf.edu.cu/index.php/rus/article/view/2888

Satterthwaite, F. E. (1946). An approximate distribution of estimates of variance components. *Biometrics Bulletin*, 2(6), 110–114. https://doi.org/10.2307/3002019

Shawe-Taylor, J., & Cristianini, N. (2004). *Kernel methods for pattern analysis*. Cambridge university press.

Shmueli, G. (2010). To explain or to predict? *Statistical Science, 25*(3), 289–310. https://doi.org/10.1214/10-STS330

Singh, K., & Best, P. (2019). Anti-money laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, 34, 100418. https://doi.org/10.1016/j.accinf.2019.06.001

Souto-Zabaleta, M., Delfino, P., & Sarti, S. S. (2019). Consideraciones críticas sobre el abordaje del problema del narcotráfico en Argentina. *Revista Ius, 13*(44), 51-88. https://doi.org/10.35487/rius.v13i44.2019.466

Stone, M. (1974). Cross-validatory choice and assessment of statistical prediction (with discussion). *Journal of the Royal Statistical Society: Series B (Methodological)*, *36*(2), 111–147.

Superintendencia de Banca, Seguros y AFP. (2015). *Reglamento de gestión de riesgos de lavado de activos y del financiamiento del terrorismo* (Resolución SBS N.º 2660-2015).

Superintendencia de Banca, Seguros y AFP. (2023). *Informe de resultados del Reporte de Operación Sospechosa de los sujetos obligados supervisados por la UIF*. Unidad de Inteligencia Financiera del Perú.

Sutton, R. S., & Barto, A. G. (2018). *Reinforcement learning: An introduction*. MIT press.

Suzumura, T., & Kanezashi, H. (2021). Anti-Money Laundering Datasets: InPlusLab anti-money laundering datasets [Dataset]. IBM. https://github.com/IBM/AMLSim

Thrun, M. C., Gehlert, T., & Ultsch, A. (2020). Analyzing the Fine Structure of Distributions. *PloS one*, 15(10), e0238835. https://doi.org/10.1371/journal.pone.0238835

Trevor, H., Tibshirani, R., & Friedman, J. (2009). *The Elements of Statistical Learning: Data Mining, Inference, and Prediction* (2a ed.). Springer,

United Nations Convention Againts Corruption. (2005). *Convención de las Naciones Unidas contra la Corrupción*. Naciones Unidas. unodc.org. Obtenido de https://www.unodc.org/unodc/en/corruption/uncac.html

United Nations Office on Drugs and Crime. (2022). *Lavado de activos*. Unodc.org. https://www.unodc.org/peruandecuador/es/02AREAS/DELITO/lavado-de-activos.html

Useche, M. C., Artigas, W., Queipo, B., & Perozo, E. (2019). *Técnicas e instrumentos de recolección de datos cuali-cuantitativos*. Universidad de la Guajira

Vaidya, J., Zhu, Y., & Clifton, C. (2006). *Privacy preserving data mining*. Springer. https://doi.org/10.1007/978-0-387-29489-6

VanderPlas, J. (2016). *Python Data Science Handbook*. O'Reilly.

Vapnik, V. (1995). *The Nature of Statistical Learning Theory*. Springer.

Weber, M., Domeniconi, G., Chen, J., Weidele, D. K. I., Bellei, C., Robinson, T., & Leiserson, C. E. (2019). *Anti-money laundering in Bitcoin: Experimenting with graph convolutional networks for financial forensics* [Conferencia]. Tutorial in the Anomaly Detection in Finance Workshop at the 25th SIGKDD Conference on Knowledge Discovery and Data Mining. https://doi.org/10.48550/arXiv.1908.02591

Welch, B. L. (1947). The generalization of "Student's" problem when several different population variances are involved. *Biometrika*, 34(1–2), 28–35. https://doi.org/10.2307/2332510

Winston, P. H. (1992). *Artificial Intelligence* (3a ed.). Pearson Educación.

Wolpert, D. H. (1996). *The lack of a priori distinctions between learning algorithms*. *Neural Computation*, 8(7), 1341–1390. https://doi.org/10.1162/neco.1996.8.7.1341

Zhang, Y., & Trubey, P. (2019). Machine learning and sampling scheme: An empirical study of money laundering detection. *Computational Economics, 54*(3), 1043–1063. https://doi.org/10.1007/s10614-018-9864-z

Zhang, Z., Zhou, X., Zhang, X., Wang, L., & Wang, P. (2018). A Model Based on Convolutional Neural Network for Online Transaction Fraud Detection. *Security and Communication Networks*, 1–9. https://doi.org/10.1155/2018/5680264

Zhu, X., & Goldberg, A. B. (2022*). Introduction to semi-supervised learning*. Springer Nature.

Zhu, X., Ghahramani, Z., & Lafferty, J. D. (2003). Semi-supervised learning using gaussian fields and harmonic functions*. In Proceedings of the 20th International conference on Machine learning* (ICML-03) (pp. 912-919). https://cdn.aaai.org/ICML/2003/ICML03-118.pdf

Zhou, Z.-H. (2012). *Ensemble methods: Foundations and algorithms* (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/b12207

ANEXOS

Anexo A. Matriz de Consistencia

Problema General	**Objetivo General**	**Hipótesis General**	**Variables/Indicadores**
¿Cómo influye la implementación de un modelo predictivo de aprendizaje automático en la detección temprana de transacciones de lavado de activos en entidades financieras?	Determinar la influencia de la implementación de un modelo predictivo de aprendizaje automático en la detección temprana de transacciones de lavado de activos en entidades financieras.	La implementación de un modelo predictivo de aprendizaje automático mejora en la detección temprana de transacciones de lavado de activos en entidades financieras.	Y: Detección de transacciones de lavado de activos. Indicador: • Hiperparámetros X_i: Modelos predictivos de aprendizaje automático Indicador: • Sensibilidad (Recall) • Precision (Precision) • Área Bajo la Curva ROC (AUC-ROC)
Problemas Específicos	**Objetivos Específicos**	**Hipótesis Específicas**	
¿Cómo influye la implementación del modelo predictivo seleccionado en la sensibilidad (Recall) para la	Determinar la influencia de la implementación del modelo predictivo seleccionado sobre la	La implementación del modelo predictivo seleccionado influye positivamente	

detección temprana de transacciones de lavado de activos en entidades financieras?	sensibilidad (Recall) en la detección temprana de transacciones de lavado de activos en entidades financieras.	en el incremento de la sensibilidad (Recall) en la detección temprana de transacciones de lavado de activos en entidades financieras.
¿Cómo influye la implementación del modelo predictivo seleccionado en la precisión (Precision) para la detección temprana de transacciones de lavado de activos en entidades financieras?	Determinar la influencia de la implementación del modelo predictivo seleccionado sobre la precisión (Precision) en la detección temprana de transacciones de lavado de activos en entidades financieras.	La implementación del modelo predictivo seleccionado influye positivamente en el incremento de precisión (Precision) en la detección temprana de transacciones de lavado de activos en entidades financieras.
¿Cómo influye la implementación	Determinar la influencia de la	La implementación

del modelo predictivo seleccionado en el área bajo la curva ROC (AUC-ROC) para la detección temprana de transacciones de lavado de activos en entidades financieras?	implementación del modelo predictivo seleccionado sobre el área bajo la curva ROC (AUC-ROC) en la detección temprana de transacciones de lavado de activos en entidades financieras.	del modelo predictivo seleccionado influye positivamente en el incremento del área bajo la curva ROC (AUC-ROC) en la detección temprana de transacciones de lavado de activos en entidades financieras.

Nota. Elaboración propia