**Logotipo

Descripción generada automáticamente**

**Mejorando la Detección de Lavado de Dinero en el Sector Financiero mediante Aprendizaje Activo**

Cristian Javier Sánchez Álvarez

Sebastián Naranjo Torres

Monografía presentada para optar al título de Especialista en Analítica y Ciencia de Datos

Asesor  
David Manuel Villanueva Valdés

Universidad de Antioquia  
Facultad de Ingeniería

Especialización en Analítica y Ciencia de Datos

Medellín, Antioquia, Colombia

2023

**Tabla de contenido**

[Resumen 4](#_heading=h.3rdcrjn)

[Abstract 5](#_heading=h.26in1rg)

[1.](#_heading=h.35nkun2) Descripción del problema 6

[1.1.](#_heading=h.1ksv4uv) Problema de negocio 6

[1.2.](#_heading=h.44sinio) Aproximación desde la analítica de datos 7

[1.3.](#_heading=h.z337ya) Origen de los datos 8

[1.4.](#_heading=h.3j2qqm3) Métricas de desempeño 9

[2.](#_heading=h.4i7ojhp) Objetivos 10

[2.1.](#_heading=h.2xcytpi) Objetivo general 10

[2.2.](#_heading=h.3whwml4) Objetivos específicos 10

[3.](#_heading=h.2bn6wsx) Datos 11

[3.1.](#_heading=h.qsh70q) Datos originales 11

[3.2.](#_heading=h.3as4poj) Datasets 12

[3.3.](#_heading=h.1pxezwc) Analítica descriptiva 15

**Lista de figuras**

**[Figura 1](#_heading=h.2r0uhxc)** [Diagrama de la Metodología CRISP-DM" 22](#_heading=h.2r0uhxc)

[**Figura 2** Vector de Alto Nivel Agregado 22](#_heading=h.1664s55)

# Resumen

El monitoreo de transacciones financieras es una obligación crítica en la lucha contra el lavado de dinero (AML) para las instituciones financieras. En los últimos años, los sistemas de monitoreo de transacciones basados en aprendizaje automático han complementado con éxito los sistemas tradicionales basados en reglas, reduciendo el alto número de falsos positivos y el esfuerzo necesario para revisar manualmente todas las alertas. Sin embargo, las soluciones basadas en aprendizaje automático también tienen desventajas: mientras que los modelos no supervisados pueden detectar nuevos patrones anómalos, generalmente se caracterizan por un alto número de falsas alarmas; los modelos supervisados, por otro lado, suelen ofrecer una mayor tasa de detección, pero requieren una gran cantidad de datos etiquetados para alcanzar dicho rendimiento. En esta primera parte de la investigación, proponemos un enfoque que integra el aprendizaje activo para la detección de anomalías, combinando técnicas de aprendizaje no supervisado y supervisado para mejorar los procesos de monitoreo de transacciones, aumentando el rendimiento de la detección y reduciendo los costos de gestión del cumplimiento. Para ello, utilizamos un conjunto de datos sintético con transacciones que simulan perfiles de clientes que operan en mercados de capitales internacionales, generando características agregadas que representan el comportamiento de los usuarios en diferentes ventanas temporales para el entrenamiento de los modelos.

*Palabras clave*: lavado de dinero, aprendizaje supervisado, aprendizaje no supervisado, aprendizaje activo.

# Abstract

Financial transaction monitoring is a critical obligation in the fight against money laundering (AML) for financial institutions. In recent years, machine learning-based transaction monitoring systems have successfully complemented traditional rule-based systems, reducing the high number of false positives and the effort needed to manually review all alerts. However, machine learning-based solutions also have drawbacks: while unsupervised models can detect new anomalous patterns, they are generally characterized by a high number of false alarms; supervised models, on the other hand, usually offer a higher detection rate but require a large amount of labeled data to achieve such performance. In this first part of the research, we propose an approach that integrates active learning for anomaly detection, combining unsupervised and supervised learning techniques to improve transaction monitoring processes, increasing detection performance, and reducing compliance management costs. To achieve this, we use a synthetic dataset with transactions that simulate profiles of clients operating in international capital markets, generating aggregated features that represent user behavior over different time windows for model training.

*Keywords: money laundering, supervised learning, unsupervised learning, active learning.*

Repositorio en GitHub: https://github.com/HerrSebas/monografia/tree/main

# Descripción del problema

## Problema de negocio

En el mundo actual, el lavado de dinero afecta a todas las economías del mundo y es responsable de generar flujos financieros ilegales entre 1,6 y 2,85 billones de dólares al año, equivalente al 2,1%-4% del Producto Bruto Mundial. Al principio, se implementaban un conjunto de reglas que estaban configuradas para monitorear comportamientos inusuales predeterminados. Estas generaban alertas, por ejemplo, si la cantidad era mayor que 10.000.000 (umbral estático), entonces se generaba una alerta. Los beneficios de este enfoque eran la facilidad para interpretar el resultado del sistema y la capacidad de los expertos en la materia (es decir, analistas que trabajan en el área de detección de anomalías) de utilizar esa información fácilmente. La desventaja es que las técnicas de lavado de dinero y los delitos financieros siempre están evolucionando, por lo que las reglas debían actualizarse para garantizar que fueran adecuadas para reflejar estos cambios. Además, las reglas solo podían cubrir comportamientos anómalos conocidos y no podían detectar comportamientos inusuales desconocidos, lo que daba lugar a falsos negativos.

El aprendizaje automático superó estas dificultades de los sistemas basados en reglas. Los modelos de aprendizaje automático pueden extraer y analizar patrones e ideas a partir de datos y evaluar correlaciones inusuales desconocidas para los expertos en la materia. Los modelos de aprendizaje automático supervisados pueden clasificar las transacciones como normales o anómalas. Sin embargo, requieren una gran muestra de transacciones revisadas manualmente (etiquetadas).

Como consecuencia de esto, actualmente las empresas del sector financiero requieren mejorar la eficacia y eficiencia en la detección de transacciones fraudulentas relacionadas con actividades de lavado de dinero mediante una recopilación del conjunto de datos etiquetados más rápida y eficiente, es decir, aprovechando el aprendizaje activo. El aprendizaje activo es una técnica que utiliza modelos de aprendizaje automático para seleccionar transacciones para una investigación que tengan la mayor probabilidad de mejorar el rendimiento del sistema de aprendizaje automático supervisado.

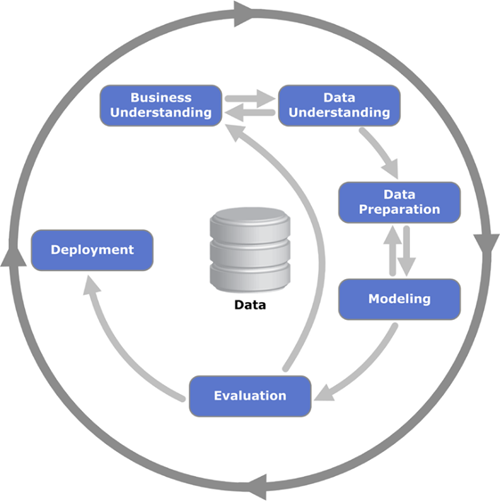
Para ello, se cuenta con una extensa base de datos transaccionales que consta de millones de transacciones ejecutadas por clientes finales que compran y venden valores específicos en un mercado.

## Aproximación desde la analítica de datos

Para abordar el problema de detección de anomalías en transacciones financieras, se seguirá un enfoque basado en la analítica de datos, utilizando modelos de aprendizaje supervisado y no supervisado. Este enfoque se llevará a cabo siguiendo la metodología CRISP-DM (Cross-Industry Standard Process for Data Mining). En la fase de comprensión del negocio, se buscará entender los objetivos y requisitos de la empresa en el ámbito de la detección de lavado de dinero, definiendo métricas de éxito y estableciendo un plan de proyecto. Luego, en la fase de comprensión de los datos, se explorarán y analizarán los datos disponibles, que consisten en transacciones financieras sintéticas generadas, identificando características relevantes y comprendiendo la estructura y distribución de los datos.

En la preparación de datos, se preprocesarán los datos de transacciones para generar características temporales y financieras que representen el comportamiento del usuario a lo largo del tiempo, agregando información en ventanas de tiempo específicas para capturar comportamientos a corto, mediano y largo plazo. En la fase de modelado, se utilizará un modelo de aprendizaje no supervisado, como el Isolation Forest, para identificar posibles anomalías basadas en las características agregadas. Con el feedback de expertos, se etiquetará un subconjunto de datos y se utilizará para entrenar un modelo de aprendizaje supervisado, específicamente un Random Forest, que clasificará las transacciones como normales o anómalas con mayor precisión.

La evaluación del rendimiento de los modelos desarrollados se realizará utilizando métricas como precisión, recall y F1-score sobre un conjunto de datos de prueba, comparando los resultados con los objetivos del proyecto y realizando ajustes según sea necesario. Finalmente, una vez validado y optimizado el modelo, se desplegará en un entorno de producción donde se integrará con los sistemas existentes de la institución financiera para la detección automatizada de actividades anómalas en tiempo real. Este enfoque proporcionará una solución robusta y adaptable para la detección eficiente de lavado de dinero en el sistema financiero, mejorando así la seguridad y la confianza en las operaciones financieras.



[Figura 1](#_heading=h.2r0uhxc): *Diagrama de la Metodología CRISP-DM*

## Origen de los datos

En el ámbito AML, una de las principales limitaciones es la dificultad de obtener un conjunto de datos real de las instituciones financieras debido a preocupaciones de privacidad. Además, es aún más complicado conseguir un conjunto de datos etiquetado. Por lo tanto, utilizamos un conjunto de datos sintéticos generado utilizando un generador de datos personalizado, que simula perfiles de transacciones de clientes que realizan transacciones en mercados de capital internacionales.

Los datos combinan más de 10.000 parámetros extrapolados de datos reales del mercado. El conjunto de datos consta de 29.704.090 transacciones ejecutadas por 400 clientes finales que compran y venden valores específicos en un mercado específico distribuidas en un periodo de 60 días dividido en 12 semanas.

## Métricas de desempeño

En la evaluación del desempeño de los modelos y su impacto en el negocio, es crucial utilizar métricas para proporcionar una visión completa de su efectividad y viabilidad.

* Precisión (Accuracy): Mide la proporción de predicciones correctas (tanto verdaderos positivos como verdaderos negativos) sobre el total de predicciones realizadas.
* Tasa de Falsos Positivos (False Positive Rate, FPR): Indica la proporción de transacciones normales que fueron clasificadas incorrectamente como anómalas. Es crucial minimizar esta tasa para evitar alarmas innecesarias.
* Tasa de Falsos Negativos (False Negative Rate, FNR): Indica la proporción de transacciones anómalas que no fueron detectadas. Reducir esta tasa es esencial para asegurarse de que las actividades fraudulentas no pasen desapercibidas.
* AUC-ROC (Área bajo la curva Receiver Operating Characteristic): Mide la capacidad del modelo para distinguir entre clases. Un AUC cercano a 1 indica un excelente desempeño del modelo.
* F1-Score: Es la media armónica de la precisión y la exhaustividad (recall), útil para evaluar el equilibrio entre falsos positivos y falsos negativos.

# Objetivos

## Objetivo general

Desarrollar un sistema de detección de lavado de dinero (AML) basado en técnicas de aprendizaje activo e integración de modelos supervisados y no supervisados, que permita identificar transacciones sospechosas en un conjunto de datos sintético del mercado de capitales.

## Objetivos específicos

* Agregar y preprocesar los datos: Recolectar y preparar el conjunto de datos sintético del mercado de capitales para su posterior análisis, incluyendo la limpieza y transformación de los datos según sea necesario.
* Implementar módulos de detección no supervisada: Desarrollar y aplicar algoritmos de detección de anomalías, como el Isolation Forest, para identificar patrones sospechosos en las transacciones financieras.
* Entrenar modelos supervisados: Utilizar técnicas de aprendizaje supervisado, como Random Forest, para entrenar modelos capaces de clasificar transacciones como normales o sospechosas, utilizando etiquetas obtenidas a través de la revisión por expertos.
* Diseñar estrategias de selección de transacciones para revisión: Desarrollar métodos de selección de transacciones basados en la combinación de resultados de los modelos supervisados y no supervisados, priorizando aquellas con mayor probabilidad de ser anómalas o con mayor discrepancia entre los modelos.
* Evaluar el rendimiento del sistema: Evaluar la efectividad del sistema de detección de lavado de dinero en la identificación de transacciones sospechosas, utilizando métricas como precisión, recall y F1-score sobre un conjunto de datos de prueba.

# Datos

## Datos originales

El dataset se distribuye en ficheros en formato CSV, organizados en columnas que contienen diferentes atributos relevantes para cada transacción. A continuación, se describe la estructura y el contenido de las columnas:

* **Transaction ID:** Identificador único de la transacción.
* **Originator:** Identificador del cliente que origina la transacción.
* **Originator\_ID:** Identificador alternativo del cliente.
* **EntryDate:** Fecha y hora en la que se registra la transacción.
* **InputOutput:** Indica si la transacción es una compra (Buy) o una venta (Sell).
* **Market:** Mercado en el cual se ejecuta la transacción.
* **Product ISIN:** Código ISIN del producto negociado.
* **Product Type:** Tipo de producto (por ejemplo, FX, FutureCommodity).
* **Product Class:** Clase de producto (por ejemplo, Trade).
* **Normalized Amount:** Monto normalizado de la transacción.
* **Currency:** Moneda en la que se realiza la transacción.
* **Anomaly:** Indicador de anomalía (0 para transacciones legítimas, 1, 2, 3, 4, 5 para transacciones anómalas).

**Etiquetado de Datos para Aprendizaje Supervisado**

Para el contexto de aprendizaje supervisado, los datos incluyen etiquetas que identifican transacciones anómalas (1,2,3,4) y legítimas (0).

* **Transacciones legítimas:** 29,622,822
* **Transacciones anómalas:** 81,262
* **Ratio de anomalías:** 0.27%

Estas anomalías se han generado sintéticamente para replicar patrones sospechosos según las directrices del Grupo de Acción Financiera Internacional (FATF).

**Descripción de Anomalías Sintéticas**

Se han generado cinco clases de anomalías basadas en patrones sospechosos comunes:

* Transacciones pequeñas, pero altamente frecuentes en un corto período de tiempo.
* Transacciones con montos redondeados dentro de una cuenta.
* Transacciones de valores a horas inusuales.
* Grandes retiros de efectivo.
* Transferencias inusualmente grandes de valores en un corto período de tiempo.

**Tamaño y Acceso a los Datos**

El dataset consta de un total de 29,704,090 registros, con un tamaño total aproximado de 3.3 GB (.CSV). Es un conjunto de datos público que puede ser encontrado en:

<https://github.com/necst/amaretto_dataset/tree/main/Data>

## Datsets

**Construcción de Datasets de Entrenamiento y Validación**

Para la construcción de los datasets de entrenamiento y validación a partir de los datos originales, generaremos un conjunto de características de alto nivel derivadas de los datos transaccionales. Estas características agregadas se basan en ventanas de agregación que capturan el comportamiento a corto, mediano y largo plazo del usuario (según se necesite). La ventana de agregación utilizada inicialmente es de 1 hora para capturar comportamientos a muy corto plazo.

**Extracción y Agregación de Características:**

**Características Temporales:**

* Se extraen características temporales a partir de la columna **EntryDate**, como el día de la semana (Weekday) y la hora (Hour).
* Además, se clasifican las transacciones en periodos del día: mañana (Morning), tarde (Evening) y noche (Night).

**Condiciones Especiales en Monto:**

* Se identifican transacciones con montos redondeados y montos pequeños específicos, considerando patrones sospechosos que pueden indicar actividades anómalas.

**Condiciones Basadas en Tipo de Transacción:**

* Se distinguen las transacciones de compra y venta, y se calcula un delta de entrada/salida (InputOutput\_Delta), que refleja la diferencia entre operaciones de compra y venta.

**Agregación de Transacciones:**

* Las transacciones se agrupan por cliente (**Originator**), día de la semana, hora y periodos del día (mañana, tarde, noche). Luego, se calculan varias estadísticas, tales como el número total de transacciones, el monto total negociado, el número de transacciones pequeñas, el número de transacciones con montos redondeados, y la identificación de transacciones anómalas.
* Dentro de cada ventana de agregación, múltiples características se extraen y agregan: total de montos negociados, monto promedio negociado, número de transacciones, número de transacciones por clase de producto, total negociado por tipo de producto para cada clase de producto y moneda, y número de transacciones durante diferentes tiempos del día.

**Limpieza de Datos:**

* Después de la agregación, se eliminan las columnas temporales utilizadas para las condiciones de agregación, asegurando que el dataset final sea limpio y eficiente para su uso en el entrenamiento y validación de modelos.

**Resultado:**

El resultado de este proceso es un conjunto de vectores de alto nivel que capturan la firma de comportamiento del usuario en cada ventana de tiempo, que están listos para ser utilizados en el módulo de detección de anomalías. Estos vectores de alto nivel contienen información agregada que refleja los patrones de comportamiento transaccional de los usuarios, facilitando la identificación de actividades inusuales.

|  |  |
| --- | --- |
| **Aggregated Features** | |
| Originator\_Client | 45 |
| Weekday | 6 |
| Hour | 9 |
| Night | 0 |
| Morning | 1 |
| Evening | 0 |
| Total\_Amount\_Traded | 3545.56 |
| Anomaly | 1 |
| Transactions\_Count\_Small\_Amount | 5 |
| Transactions\_Count\_Round\_Amount | 17 |
| Transactions\_Count\_Amount\_Sell | 50 |
| Transactions\_Count\_Amount\_Buy | 88 |
| InputOutput\_Delta | -38 |

Figura 2: *Vector de Alto Nivel Agregado*

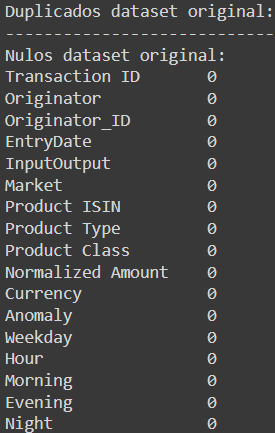
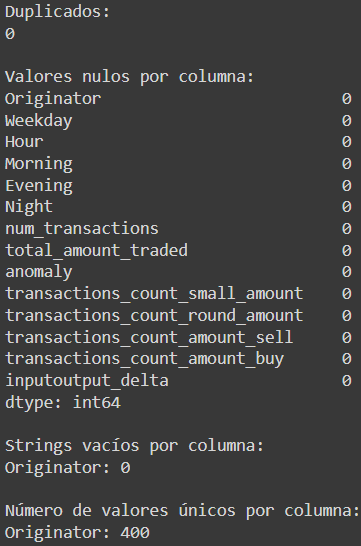
Este enfoque asegura que se puedan detectar actividades anómalas basadas en las características agregadas de las transacciones. Por otro lado, inicialmente, el 80% de los datos del dataframe agregado se utilizará para el entrenamiento, mientras que el 20% restante se destinará a la validación de los modelos.

## Analítica descriptiva

# 

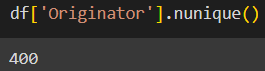
Es preciso mencionar que dentro de los datos no es posible identificar distribuciones estadísticas; sin embargo, se intentará realizar un análisis descriptivo de los datos para comprender mejor sus características principales.

**Valores nulos y duplicados en el dataset original y el dataset de entrenamiento (agregado):**

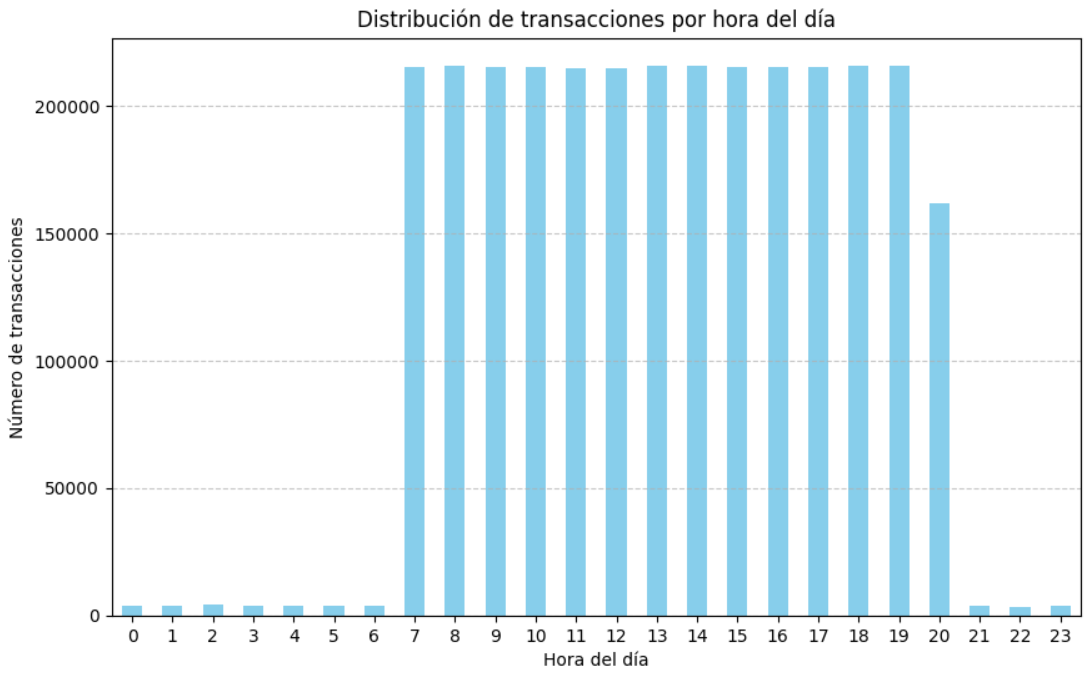
Los conjuntos de datos no poseen valores duplicados ni valores nulos.

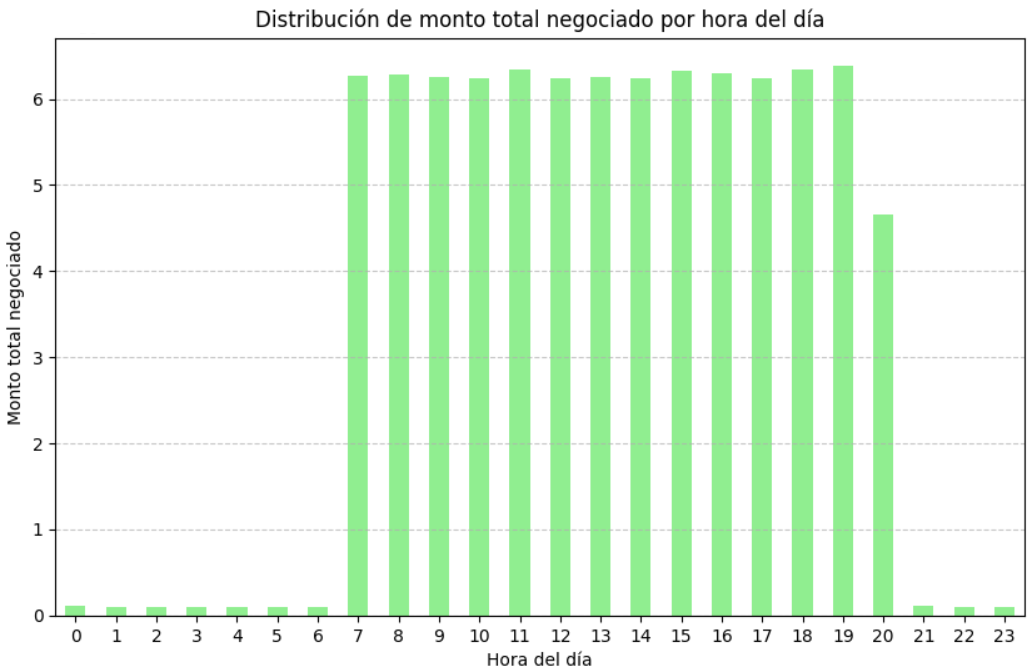
**Número de clientes:**



Este dataset consta de transacciones ejecutadas por 400 clientes finales que compran y venden valores específicos en un mercado determinado.

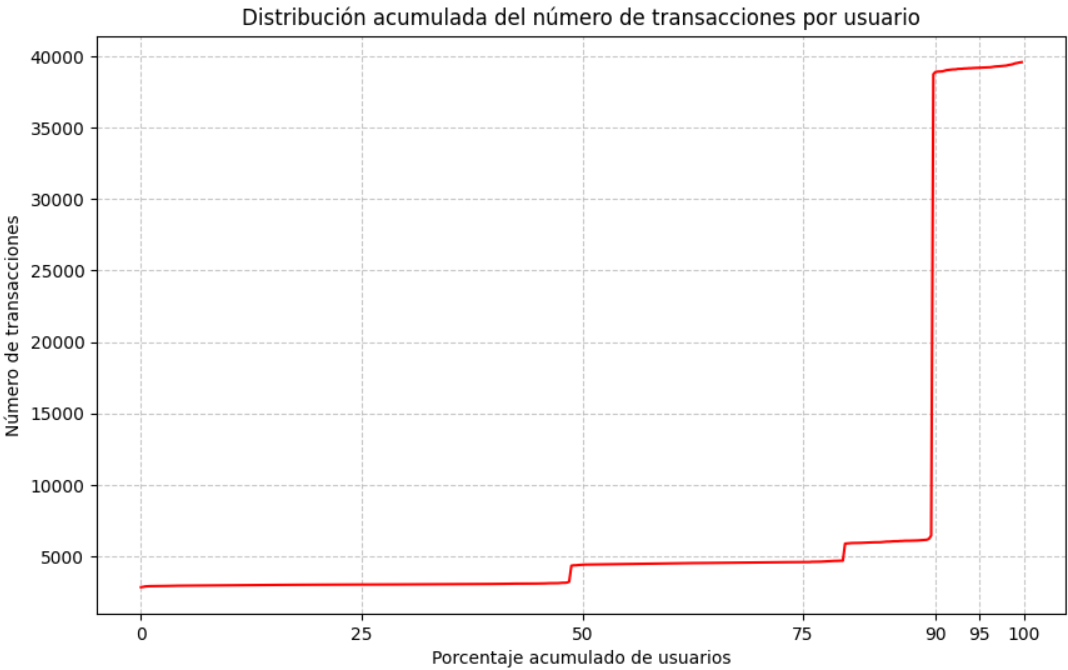
**Distribución del número de transacciones y el monto total negociado por hora del día:**





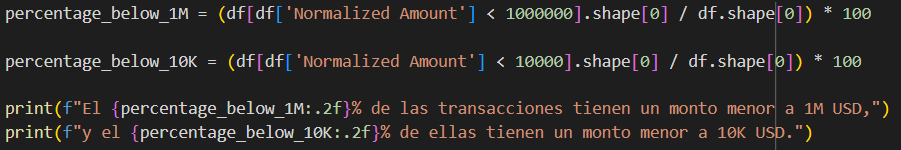
Las transacciones se distribuyen uniformemente tanto en número como en monto total negociado durante el horario de apertura del mercado, mientras que solo un pequeño porcentaje se ejecuta durante las primeras horas de la mañana y al final del día.

**Distribución del número de transacciones por usuario:**



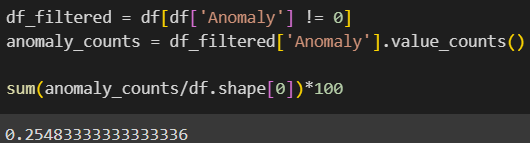
Alrededor del 90% de los usuarios realizaron al menos 5000 transacciones (en una muestra aleatoria de 3 millones de datos), mientras que el 10% de los usuarios realizó alrededor de 25000, lo que significa que el 10% de los clientes ejecutaron casi el 50% de las transacciones.

**Distribución del monto total:**

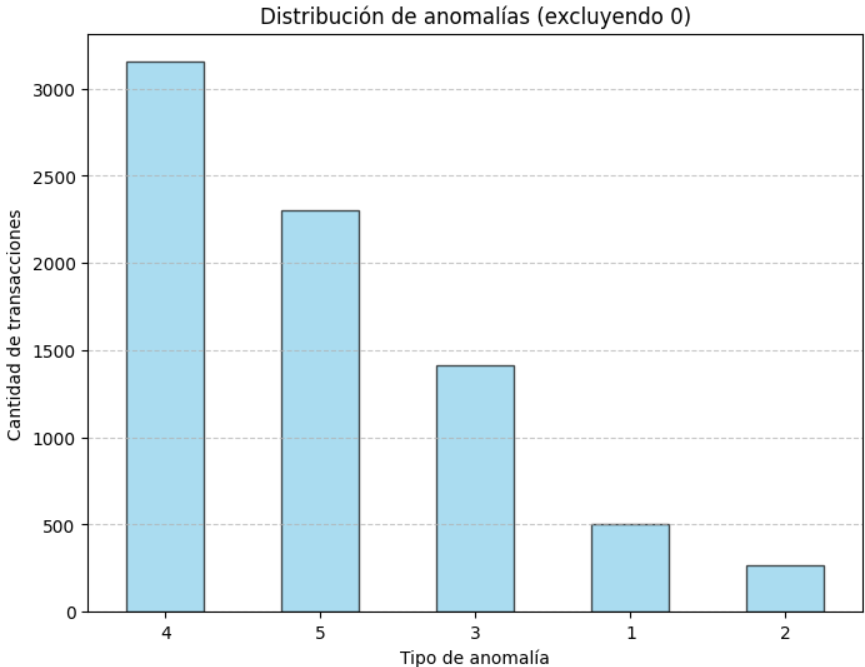


El 96.02% de las transacciones tienen un monto menor a 1M USD, y el 26.20% de ellas tienen un monto menor a 10K USD.

**Cantidad y tipos de anomalías:**



El conjunto de datos está extremadamente desbalanceado en términos de transacciones anómalas, representando solo el 0.2542% o menos del 1% del total de transacciones. Este desbalance se establece para replicar escenarios del mundo real, donde las anomalías son eventos raros y poco comunes.



De una muestra aleatoria de 3 millones de datos, se puede observar que las anomalías 4 (Grandes retiros de efectivo) y 5 (Transferencias inusualmente grandes de valores en un corto período de tiempo) son las anomalías que más se presentan.

# Referencias

United Nations Of ce on Drugs and Crime. (2011). Estimating Illicit Financial Flows Resulting From Drug Traf cking and Other Transnational Organized Crimes. [Online]. Available: https://www.unodc.org/documents/data-and-analysis/Studies/Illicit\_nancial\_ows\_2011\_web.pdf

FATF. (2018). Guidance for a Risk-Based Approach: Securities Sector. [Online]. Available: https://www.fatf-ga.org/media/fatf/documents/recommendations/pdfs/RBA-Securities-Sector.pdf

T. L. V. Barnett, Outliers in Statistical Data, 3rd ed. Hoboken, NJ, USA: Wiley, 1994.

Z. Chen, L. D. V. Khoa, E. N. Teoh, A. Nazir, E. K. Karuppiah, and K. S. Lam, Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review, Knowl. Inf. Syst., vol. 57, no. 2, pp. 245285, 2018, doi: 10.1007/s10115-017 1144-z.

M.Carminati, R. Caron, F. Maggi, I. Epifani, and S. Zanero, BankSealer: A decision support system for online banking fraud analysis and investigation, Comput. Secur., vol. 53, pp. 175186, Sep. 2015, doi: 10.1016/j.cose.2015.04.002.

N. A. L. Khac and M.-T. Kechadi, Application of data mining for anti-money laundering detection: A case study, in Proc. 10th IEEE Int. Conf. Data Mining Workshops (ICDMW), W. Fan, W. Hsu, G. I. Webb, B. Liu, C. Zhang, D. Gunopulos, and X. Wu, Eds. Sydney, NSW, Australia: IEEE Computer Society, Dec. 2010, pp. 577584, doi: 10.1109/ICDMW.2010.66.

R. A. L. Torres and M. Ladeira, A proposal for online analysis and identification of fraudulent financial transactions, in Proc. 19th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA), M. A. Wani, F. Luo, X. A. Li, D. Dou, and F. Bonchi, Eds., Miami, FL, USA, Dec. 2020, pp. 240245, doi: 10.1109/ICMLA51294.2020.00047.