Detección de transacciones anómalas como herramienta de gestión del riesgo operativo

Anthony Jiménez[1], Gustavo Amador[2]
Javier Hernández[3], Luis Amey[4]
Johan Castaño[5]

[1] Escuela de Matemática, Universidad de Costa Rica, San José, 11501, Costa Rica
anthony.jimeneznavarro@ucr.ac.cr

[2] Escuela de Matemática, Universidad de Costa Rica, San José, 11501, Costa Rica
gustavo.amadorfonseca@ucr.ac.cr

[3] Escuela de Matemática, Universidad de Costa Rica, San José, 11501, Costa Rica
javier.hernandeznavarro@ucr.ac.cr

[4] Escuela de Matemática, Universidad de Costa Rica, San José, 11501, Costa Rica
luis.amey@ucr.ac.cr

[5] Escuela de Matemática, Universidad de Costa Rica, San José, 11501, Costa Rica
johan.castano@ucr.ac.cr

5 de diciembre de 2025

Resumen

La gestión del riesgo operativo constituye un componente esencial dentro del marco de los riesgos financieros, dada su capacidad de afectar la estabilidad, continuidad y reputación de las entidades. Este estudio propone un enfoque analítico orientado a la detección temprana de transacciones anómalas como medida de mitigación frente a eventos de pérdida operativa. A partir del análisis de datos transaccionales, se busca identificar patrones de comportamiento irregulares que puedan asociarse a errores operativos o a actividades fraudulentas, fortaleciendo los mecanismos de control interno y supervisión. El enfoque propuesto utiliza técnicas de aprendizaje automático para adaptar dinámicamente los criterios de identificación de anomalías, mejorando la capacidad de respuesta ante incidentes emergentes. En conjunto, este proyecto ofrece una herramienta complementaria para la gestión del riesgo operativo, integrando la analítica de datos dentro de las estrategias de prevención y mitigación de pérdidas en las instituciones financieras.

Keywords — Riesgo operativo, riesgos financieros, detección de anomalías, aprendizaje automático, fraude transaccional, control interno, mitigación de riesgos.

Índice

1. Introducción

En el marco de los riesgos financieros, el riesgo operativo ocupa un papel determinante por su capacidad de afectar simultáneamente la estabilidad económica, la continuidad del negocio y la confianza de los usuarios. Este riesgo se manifiesta como consecuencia de fallos en los procesos internos, errores humanos, deficiencias tecnológicas o eventos externos, y puede originar pérdidas significativas tanto financieras como reputacionales. A diferencia de los riesgos de crédito o de mercado, el riesgo operativo posee un carácter transversal que lo convierte en un desafío constante para las entidades financieras, especialmente en contextos de alta digitalización y creciente complejidad transaccional.

En la actualidad, las instituciones financieras procesan millones de transacciones diarias a través de múltiples canales, lo que incrementa exponencialmente la probabilidad de que ocurran eventos anómalos, ya sea por errores operativos o por actos fraudulentos. Este escenario plantea una interrogante clave:

¿Cómo pueden las entidades financieras anticipar y mitigar de forma efectiva los eventos de riesgo operativo derivados de irregularidades en las transacciones?

Frente a este desafío, las herramientas de análisis de datos y las metodologías de aprendizaje automático ofrecen una alternativa innovadora para fortalecer la detección temprana de comportamientos atípicos, permitiendo a las organizaciones responder con mayor eficacia ante potenciales pérdidas.

El presente trabajo se orienta al fortalecimiento de la gestión del riesgo operativo, concebido como una parte estratégica del marco general de riesgos financieros que enfrentan las entidades, y tiene como finalidad proponer un enfoque analítico que contribuya a la identificación y mitigación de eventos de pérdida. En particular, se plantea el uso de un modelo de detección de anomalías como medida preventiva orientada a mejorar los mecanismos de monitoreo y control. Este enfoque busca no solo identificar transacciones irregulares, sino también ofrecer evidencia empírica que respalde decisiones informadas en materia de gestión de riesgos, fortaleciendo así la resiliencia operativa y la seguridad institucional.

2. Objetivos

Para este proyecto se tiene como objetivo principal fortalecer la gestión del riesgo operativo dentro del marco de los riesgos financieros, mediante la implementación de un enfoque analítico que permita detectar tempranamente transacciones inusuales y reducir la probabilidad de pérdidas operativas. Este objetivo pretende incorporar la analítica de datos como una herramienta estratégica de mitigación, orientada a mejorar los procesos de control, supervisión y respuesta frente a eventos de riesgo que puedan comprometer la estabilidad de las entidades financieras.

Objetivos específicos

1. Identificar los factores y procesos asociados al riesgo operativo que influyen en la aparición de irregularidades dentro de las operaciones financieras.
2. Analizar la información transaccional para caracterizar patrones de comportamiento y establecer criterios que permitan distinguir operaciones normales de aquellas potencialmente anómalas.
3. Evaluar los resultados obtenidos del enfoque analítico propuesto, destacando su efectividad como medida de mitigación del riesgo operativo y su potencial aplicación dentro de los sistemas de control interno de las entidades financieras.

3. Marco teórico

Normativa de Costa Rica

En apoyo a la Ley N.º 8204 sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo, la Superintendencia General de Entidades Financieras (SUGEF) emitió el *Acuerdo SUGEF 13-19*. Este reglamento define las responsabilidades y obligaciones de los sujetos obligados en la administración del riesgo de legitimación de capitales, financiamiento al terrorismo y financiamiento de la proliferación de armas de destrucción masiva (LC/FT/FPADM), con base en el principio de gestión basada en riesgo [30, 4].

Particularmente, los artículos 36 y 37 del Acuerdo establecen la obligación de realizar procesos de monitoreo continuo y clasificación de clientes, con el fin de asegurar que el perfil transaccional de cada cliente sea coherente con la información declarada y con su categoría de riesgo. Los Lineamientos Generales del mismo acuerdo complementan esta disposición, precisando que las entidades deben identificar y analizar las señales de alerta que resulten del proceso de monitoreo para detectar situaciones inusuales y reportar aquellas que sean catalogadas como sospechosas [30].

Desde la perspectiva de la gestión integral del riesgo, el cumplimiento de estas obligaciones regulatorias implica también una dimensión operativa. Las deficiencias en los procesos de monitoreo, análisis o reporte de operaciones inusuales constituyen fuentes potenciales de riesgo operacional, al reflejar fallas en los controles internos, en los sistemas tecnológicos o en la supervisión del personal. Este tipo de debilidades puede, a su vez, amplificar otros riesgos asociados, tales como el riesgo reputacional por el deterioro de la confianza pública y el riesgo legal, derivado de sanciones o procesos por incumplimiento normativo [29, 31].

Con el fin de mitigar estos riesgos, la incorporación de herramientas analíticas y modelos de aprendizaje automático se plantea como un control operativo preventivo. Estas metodologías fortalecen la capacidad de las entidades para identificar de

forma temprana y precisa comportamientos atípicos en las transacciones, reduciendo la probabilidad de errores humanos, omisiones o demoras. De esta manera, el uso de modelos de detección de anomalías contribuye directamente a disminuir la exposición al riesgo operacional y, de forma indirecta, a los riesgos de legitimación de capitales, legales y reputacionales [31, 30].

De acuerdo con el Acuerdo SUGEF 1-05: Gestión Integral de Riesgos, las entidades deben establecer mecanismos que integren la identificación, medición, control y monitoreo de todos los riesgos a los que están expuestas. En este marco, la adopción de soluciones analíticas avanzadas favorece una gestión más eficiente y proactiva del riesgo operacional, al tiempo que consolida una cultura institucional orientada al cumplimiento y la transparencia [29, 31].

Fundamentos estadístico–teóricos

3.0.1. Z-score

El Z-score es una medida estadística que indica qué tan lejos está un valor respecto al promedio, expresado en unidades de desviación estándar. Este se expresa de la forma:

$$z = \frac{x - \mu}{\sigma},$$

con x la observación, μ el promedio de los datos y σ la desviación estándar, que representa cuánto varían los valores alrededor del promedio. De esta forma, si un valor tiene un Z-score igual a cero, significa que está justo en el promedio; si es positivo, está por encima del promedio; y si es negativo, está por debajo.

Con el Z-score se busca comparar valores que provienen de diferentes escalas o unidades. Según [11], esta transformación también permite comparar distintos tipos de medidas, como rendimiento, estado de ánimo, entre otro.

En datos temporales, como en las series de tiempo, usar el Z-score permite hacer mejores comparaciones entre diferentes variables. [8] mencionan que, cuando se normalizan las series usando el Z-score, facilita visualizar patrones y relaciones. Por otro lado, en el ámbito financiero, el Z-score ha tenido un papel importante para medir el riesgo. Lo desarrollado por [2] usa varios indicadores financieros, como liquidez y rentabilidad, para calcular un puntaje que permite anticipar la posibilidad de quiebra. Además, [21] utilizan una adaptación de lo desarrollado por [2] para medir qué tan lejos está un banco de llegar a una situación de insolvencia.

En la detección de anomalías en transacciones, el z-score es uno de los métodos rápidos para identificar movimientos atípicos. [25] desarrollan una regla de "—Z— ¿3" sobre características estandarizadas para marcar transacciones que se alejan mucho del comportamiento normal. Igualmente, [16] utilizan el z-score en combinación con técnicas de agrupamiento (como DBSCAN) para detectar casos inusuales en procesos de compras empresariales. De manera similar, [14]) usa el z-score como umbral simple en sistemas de detección, esto como primer filtro.

3.0.2. Isolation Forest

El Isolation Forest es según [23] una técnica moderna no supervisada utilizada para detectar anomalías en conjuntos de datos grandes, además, de ser muy util debido a su no necesidad de saber de antemano qué es normal o anómalo. El autor menciona que los datos que se comportan de manera diferente al resto pueden aislarse más rápidamente al dividir el espacio de datos en ramas o árboles, esto mediante la construcción de muchos árboles de forma aleatoria, eligiendo en cada uno una variable y un punto de corte también aleatorios. Si una observación necesita pocas divisiones para quedar separada de las demás, es una anomalía. En cambio, los datos normales requieren más divisiones para aislarse. Con lo cual, esta longitud representa una medida de qué tan anómalo es.

En el ámbito financiero, [32] aplicaron el Isolation Forest para detectar fraudes con tarjetas de crédito y demostraron que el modelo logra identificar operaciones sospechosas de manera efectiva, incluso con grandes volúmenes de datos. De la misma manera, [6] utilizó este enfoque para encontrar transacciones atípicas en sistemas de pago de alto valor, mostrando su capacidad para analizar flujos complejos en tiempo real. Por ultimo, [34] lo aplicaron en lo relacionado con el *blockchain*, sumado con modelos basados en grafos para detectar patrones irregulares de actividad.

3.0.3. Random Forest Classifier

El Random Forest Classifier es según [10] un algoritmo de aprendizaje supervisado que se utiliza para tareas de clasificación y detección de anomalías. Se basa en la creación de un conjunto de árboles de decisión independientes, conocidos como un "bosque aleatorio". Cada árbol se entrena con una muestra distinta de los datos y con un subconjunto aleatorio de variables en cada división. De esta manera, cada árbol aprende un patrón diferente y, al combinarse todos sus resultados, el modelo obtiene una predicción más estable y precisa.

En el contexto de detección de anomalías, el Random Forest Classifier según [5] ha mostrado muy buen desempeño, esto ya que, apartir de su investigación los autores desarrollaron un sistema de detección de fraudes con tarjetas de crédito y encontraron que su precisión supera a la de otros clasificadores tradicionales, como la regresión logística o las redes neuronales simples. De igual manera, [33] utilizaron este modelo para el caso de transacciones bancarias y lograron detectar patrones de comportamiento sospechoso con altos niveles de exactitud.

Por lo tanto, el Random Forest Classifier se puede considerar una metodología robusta y flexible para problemas de clasificación y detección de irregularidades. Su capacidad para combinar aleatoriedad, múltiples perspectivas lo convierten en una de las herramientas más confiables dentro del aprendizaje automático aplicado a transacciones financieras y análisis de riesgos.

3.0.4. Autoencoder

El Autoencoder es según [17] un tipo de red neuronal que se entrena para aprender una "codificación" de los datos. Su estructura viene dada por 2 partes: un codificador (*encoder*) que transforma los datos originales en una representación comprimida de menor dimensión, y un decodificador (*decoder*) que intenta reconstruir la entrada original a partir de esa representación interna. El objetivo del entrenamiento es minimizar la diferencia entre los valores de entrada y los valores reconstruidos.

El Autoencoder es usado en la detección de anomalías según [35] debido a que este se puede interpretar aparir del error de reconstrucción. Cuando se entrena el modelo únicamente con observaciones normales, aprende a reproducir correctamente ese comportamiento típico. Sin embargo, si se le presenta un dato inusual o anómalo, su estructura interna no logra reconstruirlo con precisión, produciendo un error de reconstrucción significativamente mayor. Por lo tanto, las observaciones cuyo error de reconstrucción supera un umbral definido se clasifican como posibles anomalías.

Por otro lado, con respecto a la detección de fraudes y anomalías en transacciones, [26] menciona el uso de los Autoencoders para analizar patrones de comportamiento financiero y descubrir operaciones atípicas, esto mediante la aplicación de un modelo basado en Autoencoder para detectar fraudes con tarjetas de créditos logrando una alta precisión en la identificación de transacciones sospechosas. De manera similar, [27] utilizan el Autoencoder a los flujos de pago, logrando que el modelo aprendiera a reconocer la estructura de las operaciones diarias y a detectar automáticamente desviaciones en el comportamiento de los participantes. Por ultimo, [35] ha implementado modelos con Autoencoder en pagos digitales apartir de modelos de aprendizaje profundo para reconocer patrones de fraude complejos y evolutivos.

4. Descripción de los datos

El conjunto de datos a utilizar ofrece una mirada detallada al comportamiento transaccional y a los patrones de actividad financiera, adecuado para el modelado de detección de fraudes e identificación de anomalías. Contiene 2,512 registros con múltiples características de las transacciones, demografía de clientes y comportamiento de uso, de modo que cada observación contribuye para el análisis de seguridad financiera y fraude. Es especialmente útil para científicos de datos, analistas financieros e investigadores interesados en analizar patrones transaccionales, detectar fraudes y construir modelos predictivos, específicamente orientado a tareas de aprendizaje automático y análisis de comportamiento [20].

- **Archivo:** `bank_transactions_data_2.csv`.
- **Tamaño:** 2,512 observaciones y 16 variables.
- **Calidad:** Ausencia de valores faltantes.

- **Variables.**
  - `TransactionID` (Identificador)
  - `AccountID` (Identificador)
  - `TransactionAmount` (Numérica)
  - `TransactionDate` (Fecha)
  - `TransactionType` (Categórica)
  - `Location` (Categórica)
  - `DeviceID` (Identificador)
  - `IP Address` (Identificador)
  - `MerchantID` (Identificador)
  - `Channel` (Categórica)
  - `CustomerAge` (Numérica)
  - `CustomerOccupation` (Categórica)
  - `TransactionDuration` (Numérica)
  - `LoginAttempts` (Numérica)
  - `AccountBalance` (Numérica)
  - `PreviousTransactionDate` (Fecha)

Resumen estadístico de las variables numéricas

La Tabla 1 presenta las principales medidas descriptivas de las variables numéricas incluidas en la base de datos. Se observa una marcada dispersión en los montos y saldos de cuenta, lo que sugiere una heterogeneidad considerable en los comportamientos financieros de los clientes. Asimismo, el número de intentos de inicio de sesión se mantiene bajo, lo cual es coherente con un patrón operativo normal.

Variable	**Media**	**DE**	**Mín**	**Mediana**	**Máx**
TransactionAmount	297,594	291,946	0,260	211,140	1.919,110
TransactionDuration	119,643	69,964	10,000	112,500	300,000
LoginAttempts	1,125	0,603	1,000	1,000	5,000
AccountBalance	5.114,303	3.900,942	101,250	4.735,510	14.977,990
CustomerAge	44,674	17,792	18,000	45,000	80,000

Cuadro 1: Resumen estadístico de variables numéricas.

En términos generales, las variables monetarias presentan distribuciones asimétricas con valores extremos, indicativos de transacciones de alta magnitud o cuentas con saldos considerablemente elevados. Este comportamiento podría asociarse a clientes corporativos o a eventos operativos puntuales. La edad promedio de los

clientes (44,7 años) refleja una población económicamente activa y diversa, lo que refuerza la necesidad de segmentar el riesgo por tipo de cliente y nivel de actividad.

Por otro lado, la Tabla 2 muestra la distribución de las operaciones según su naturaleza contable. Se observa un predominio de transacciones de débito (77,4 %), lo que sugiere un patrón de uso centrado en pagos, retiros o transferencias salientes.

Categoría	**%**
Débito	77,4 %
Crédito	22,6 %

Cuadro 2: Distribución por tipo de transacción.

En la Tabla 3 se evidencia una distribución equilibrada entre los canales *sucursal*, *cajero automático* y *en línea*, con porcentajes muy similares. Este equilibrio indica que la base de datos recoge información representativa de diferentes entornos operativos, lo que facilita el análisis comparativo de riesgo por canal.

Categoría	**%**
Sucursal	34,6 %
Cajero automático	33,2 %
En línea	32,3 %

Cuadro 3: Distribución por canal de transacción.

Asimismo, la Tabla 4 muestra una distribución homogénea entre las distintas categorías ocupacionales, con ligeras variaciones entre grupos. La presencia de perfiles profesionales y estudiantes indica una base de clientes diversa, lo que contribuye a la robustez del análisis de riesgo.

Categoría	**%**
Estudiante	26,2 %
Doctor	25,1 %
Ingeniero	24,9 %
Jubilado	23,8 %

Cuadro 4: Distribución por ocupación del cliente.

La Tabla 5 presenta la frecuencia de las transacciones según la hora del día. Se aprecia una concentración significativa en las horas vespertinas, lo que podría asociarse con los horarios habituales de pago, transferencias o consumo diario.

Hora	%
16:00	52,4 %
17:00	32,6 %
18:00	15,0 %

Cuadro 5: Distribución horaria de las transacciones.

Por último, la Tabla 6 muestra las diez ciudades con mayor número de transacciones registradas. Se observa una distribución equilibrada entre distintas regiones urbanas, sin concentración marcada en un solo punto geográfico, lo que sugiere una cartera diversificada.

Ciudad	%
Fort Worth	2,8 %
Los Ángeles	2,7 %
Oklahoma City	2,7 %
Charlotte	2,7 %
Tucson	2,7 %
Filadelfia	2,7 %
Omaha	2,6 %
Miami	2,5 %
Detroit	2,5 %
Houston	2,5 %

Cuadro 6: Principales ubicaciones geográficas de transacciones.

Al analizar la Figura 1, se puede observa la distribución del número de registros por cuenta. La mayoría de las cuentas presenta entre tres y seis operaciones, lo que refleja un comportamiento transaccional regular. Sin embargo, la presencia de algunas cuentas con más de diez registros sugiere posibles concentraciones inusuales de actividad, que podrían asociarse con errores operativos o patrones atípicos de uso.

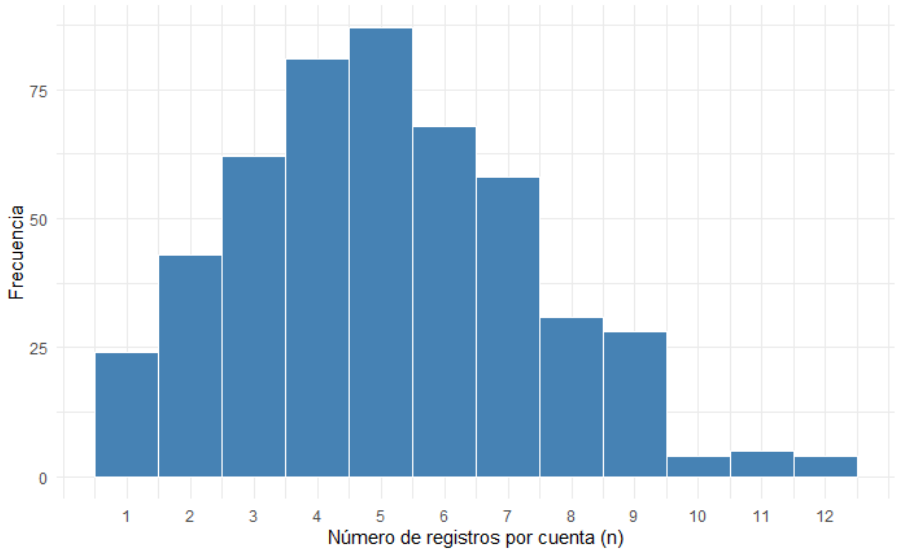

Figura 1: Histograma del número de registros por cuenta.

Fuente: Elaboración propia.

En la Figura 2 se observa la distribución de los montos de transacción, caracterizada por una asimetría positiva pronunciada. La mayoría de las operaciones corresponde a montos bajos, mientras que unas pocas transacciones de alto valor conforman una "cola larga". Este comportamiento es típico en contextos financieros minoristas y representa un punto de atención en la gestión del riesgo operativo, dado que las operaciones de gran cuantía pueden implicar exposiciones elevadas o eventos anómalos.

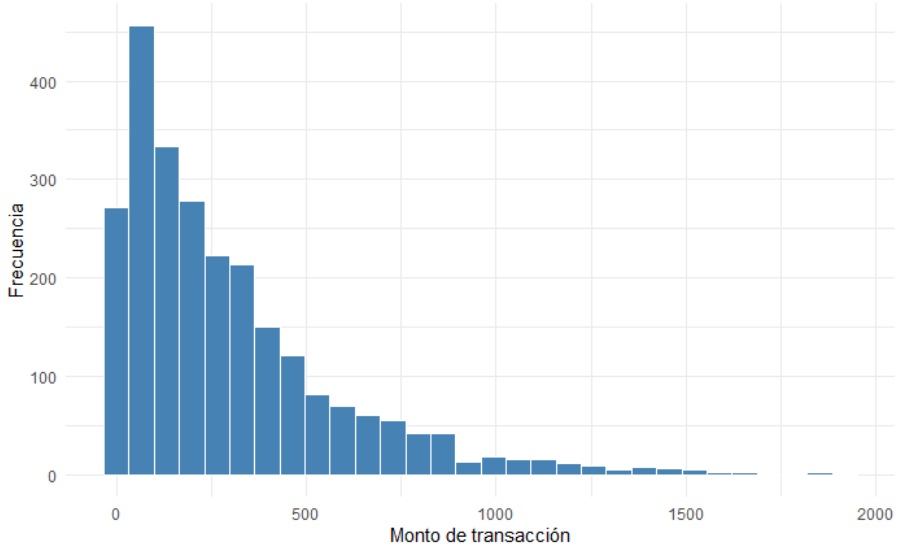

Figura 2: Histograma de las cantidades de transacciones.

Fuente: Elaboración propia.

En conjunto, las características descriptivas de la base de datos reflejan una estructura de clientes heterogénea, con operaciones distribuidas en distintos canales,

horarios y ubicaciones. Esta diversidad es crucial para el análisis de riesgo operativo, ya que permite identificar segmentos específicos donde podrían concentrarse anomalías o eventos de pérdida potencial.

5. Metodología

El enfoque metodológico implementado se desarrolló íntegramente en `R`, aplicando un proceso analítico no supervisado orientado a la detección de transacciones anómalas, con el fin de fortalecer la capacidad preventiva asociada al riesgo operativo.

5.1. Preparación de los datos

Se cargó un conjunto de datos sintético con múltiples atributos financieros (monto, saldo disponible, tipo de operación, entre otros). Inicialmente se verificó la integridad del conjunto (ausencia de valores perdidos) y se procedió a la extracción de las dos variables de mayor relevancia operativa para este primer ejercicio:

- **Monto de transacción (`TransactionAmount`)** – magnitud de la operación.
- **Saldo disponible (`AccountBalance`)** – capacidad financiera del usuario.

Ambas variables fueron estandarizadas mediante Z-score:

$$Z_i = \frac{x_i - \bar{x}}{s}$$

lo cual normaliza las escalas e impide que los modelos basados en distancia o partición sean afectados por diferencias de magnitud.

5.2. Modelado y técnicas aplicadas

1. **Detección estadística univariada — Z-score**
   Se implementó un umbral clásico de valores extremos. Si $|Z_i| > 3$, la observación fue marcada como atípica. Este método responde al supuesto de cola normal y sirve como línea base comparativa.
2. **Isolation Forest**
   Algoritmo basado en aislamiento aleatorio: las observaciones que son separadas tras pocas particiones son consideradas anomalías. El código implementa:
   - construcción de 100 árboles aisladores,
   - cálculo del *anomaly score* por cada transacción,
   - selección de anomalías mediante un `cutoff` calibrado para aproximar un 5 % de marcajes.

3. **Autoencoder**
   Se diseñó una red neuronal *encoder-decoder* con función de pérdida MSE. El entrenamiento se realizó únicamente con patrones frecuentes, de modo que:

$$\text{Anomalía si MSE}(x, \hat{x}) > \tau$$

   donde τ fue determinado mediante inspección del cuantil superior de la distribución de errores de reconstrucción.

5.3. Ajuste de umbrales y control de tasa de alertas

Para garantizar coherencia operativa, los umbrales de los tres métodos se calibraron para mantener una tasa cercana al 5 % de marcajes. Esta cifra se fundamenta en:

- frecuencia esperada de eventos relevantes en monitoreo operativo,
- necesidad de evitar sobrecarga cognitiva en analistas de riesgo,
- alineamiento con prácticas de gestión de alertas iniciales en AML.

Luego, el código asignó la etiqueta `IsAnomaly = TRUE/FALSE` por cada método y generó tres clasificaciones independientes. Posteriormente, se integraron en una matriz de coincidencias para análisis de intersecciones.

6. Resultados

Los resultados permiten evaluar la capacidad de las técnicas no supervisadas de detección de anomalías para apoyar la gestión del riesgo operativo en un entorno transaccional. En particular, se analiza cómo cada enfoque resalta patrones atípicos en el plano definido por el monto de la transacción y el saldo disponible en cuenta, variables que suelen ser críticas en los modelos de monitoreo y prevención de operaciones inusuales.

6.1. Distribución espacial de las anomalías

La Figura 3 muestra la nube de puntos de todas las transacciones, donde el eje horizontal corresponde al monto transaccional (*Transaction Amount*) y el eje vertical al saldo disponible en cuenta (*Account Balance*). Los puntos se colorean según la etiqueta generada por el criterio de Z-score, de forma que las observaciones marcadas como anómalas corresponden a valores extremos con respecto a la distribución global de la variable, típicamente aquellos por encima de un umbral absoluto de tres desviaciones estándar [19, 7].

En esta primera aproximación se aprecia que el método estadístico tiende a resaltar principalmente transacciones de monto elevado, muchas de ellas asociadas

a saldos relativamente bajos. Desde una perspectiva de riesgo operativo, este tipo de combinaciones podría vincularse tanto con errores de digitación o parametrización de montos como con intentos de sobregiro o manipulación de límites operativos.

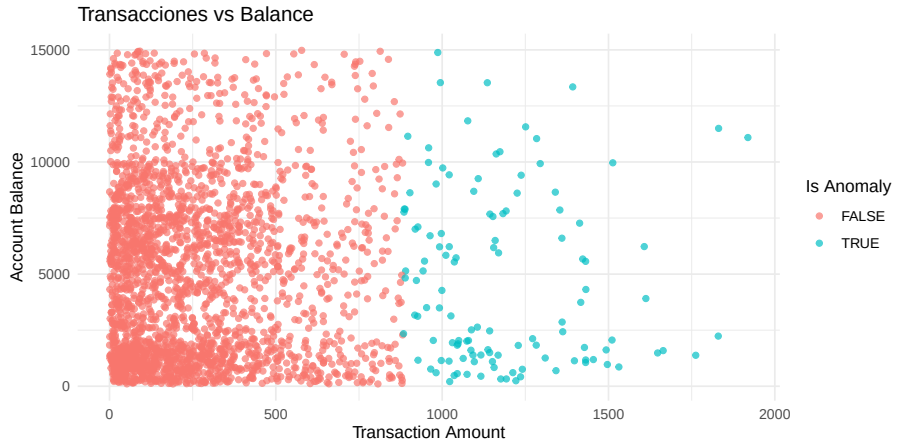

Figura 3: Anomalías detectadas mediante Z-score.

Fuente: Elaboración propia.

La Figura 4 presenta la misma nube de puntos, pero ahora con la etiqueta de anomalía generada por el algoritmo *Isolation Forest*. A diferencia del enfoque puramente univariante, este modelo considera de manera conjunta la estructura del espacio de variables, aislando de forma más eficiente aquellas observaciones que requieren pocas particiones para separarse del resto.

En la figura se observa que las anomalías no se restringen únicamente a montos extremos, sino que aparecen también en regiones donde las combinaciones de monto y saldo son poco frecuentes. Esto sugiere que el método es capaz de capturar relaciones más sutiles entre ambas variables, lo cual es especialmente útil en contextos donde los eventos operativos relevantes no siempre se manifiestan como outliers evidentes en una sola dimensión [16, 6].

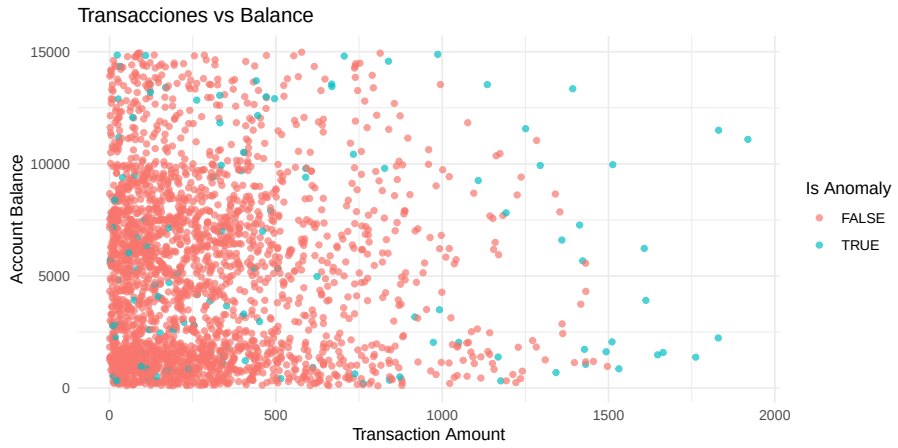

Figura 4: Anomalías detectadas mediante Isolation Forest.

Fuente: Elaboración propia.

La Figura 5 corresponde a la detección realizada con el Autoencoder. En este caso, las observaciones con errores de reconstrucción más elevados son etiquetadas como anómalas.

Visualmente, el patrón resultante es muy similar al de Figura 4, lo cual indica que tanto Isolation Forest como el Autoencoder coinciden en identificar una franja de transacciones que, sin ser necesariamente extremas en términos univariados, presentan combinaciones de monto y saldo poco compatibles con la dinámica general del conjunto. Este acuerdo entre métodos de naturaleza distinta refuerza la hipótesis de que se trata de casos operativamente relevantes, susceptibles de ser priorizados para revisión por las unidades de riesgo y cumplimiento [26, 27].

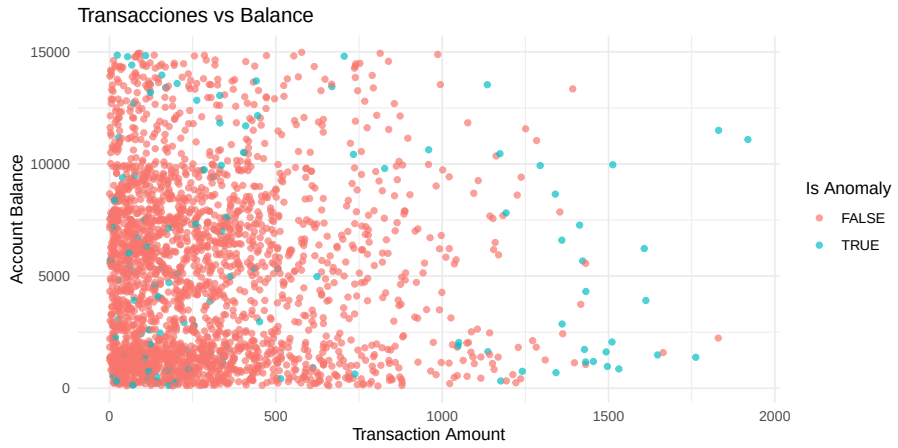

Figura 5: Anomalías detectadas mediante el Autoencoder.

Fuente: Elaboración propia.

6.2. Intersección entre modelos y priorización de alertas

Con el fin de evaluar el grado de consistencia entre los diferentes enfoques, se construyó un gráfico de intersecciones tipo *UpSet* que resume cuántas observaciones son clasificadas como anómalas por cada combinación de modelos. La Figura 6 muestra, en el eje horizontal, los distintos grupos definidos por la pertenencia o no de cada transacción a los conjuntos de anomalías de Z-score, Isolation Forest y Autoencoder; el eje vertical indica el tamaño de cada intersección.

El resultado más relevante es que la mayoría de las observaciones se agrupa en el conjunto donde ningún modelo marca anomalía, lo cual es consistente con la baja frecuencia esperada de eventos operativos significativos. En segundo lugar, destaca un subconjunto de transacciones que son señaladas simultáneamente por Isolation Forest y el Autoencoder, mientras que el aporte exclusivo de Z-score es relativamente menor.

Desde el punto de vista de la gestión del riesgo operativo, este análisis sugiere una estrategia de priorización natural: las transacciones que aparecen como anómalas en al menos dos modelos pueden considerarse candidatas prioritarias para revisión detallada, mientras que aquellas detectadas por un único algoritmo podrían destinarse a monitoreo o análisis complementario antes de escalarse [1, 13].

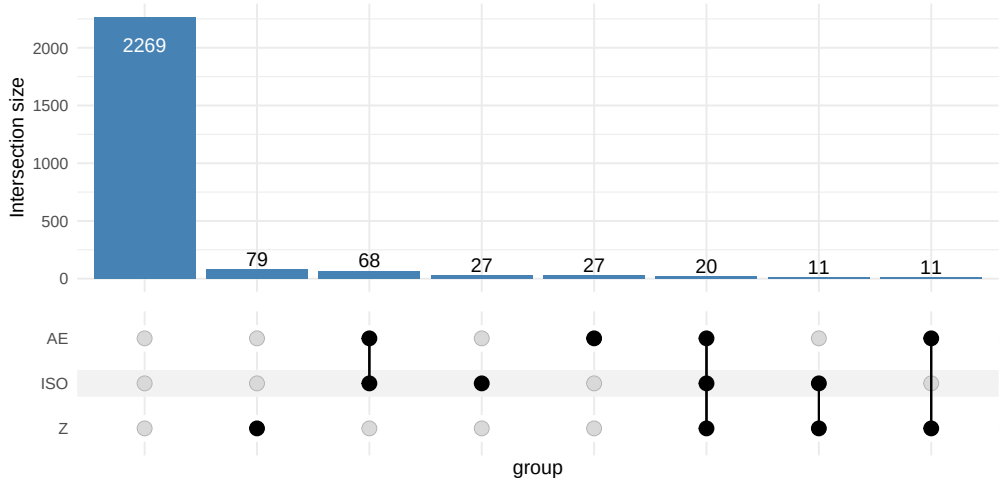

Figura 6: Intersección de anomalías detectadas por modelo.

Fuente: Elaboración propia.

7. Discusión

Los hallazgos obtenidos confirman que los enfoques no supervisados de detección de anomalías pueden aportar valor agregado a los esquemas tradicionales de control, especialmente cuando se utilizan de forma complementaria. El método de Z-score, apoyado en criterios clásicos de outliers, resulta útil como referencia base y permite identificar rápidamente valores extremos evidentes. Sin embargo, sus limitaciones

para capturar relaciones multivariantes justifican la incorporación de modelos más flexibles.

En particular, Isolation Forest y el Autoencoder logran resaltar patrones que no se caracterizan únicamente por montos exageradamente altos o bajos, sino por combinaciones atípicas de monto y saldo, coherentes con escenarios como errores de proceso, intentos de fraccionamiento de operaciones o comportamientos inusuales de ciertos segmentos de clientes. Esto se alinea con las exigencias de la normativa costarricense en materia de gestión integral de riesgos y prevención de operaciones inusuales, que enfatiza la importancia de contar con herramientas tecnológicas capaces de detectar conductas atípicas de manera oportuna.

No obstante, los resultados también ponen de manifiesto la necesidad de mantener un rol activo del análisis humano. La discrepancia entre modelos y la posibilidad de generar falsas alarmas implica que las salidas de estos algoritmos deben interpretarse como insumos para la toma de decisiones, y no como mecanismos automatizados de bloqueo o sanción.

8. Conclusiones

A partir del ejercicio desarrollado, se pueden extraer las siguientes conclusiones principales:

- La detección no supervisada de anomalías constituye una herramienta prometedora para la identificación temprana de eventos vinculados con el riesgo operativo en contextos transaccionales, complementando los controles y reportes tradicionales.
- Los modelos multivariantes, como Isolation Forest y el Autoencoder, exhiben una mayor capacidad para capturar comportamientos atípicos complejos que los enfoques univariantes basados únicamente en Z-score, lo que resulta especialmente relevante en entornos donde la interacción entre variables financieras es crítica.
- El análisis de intersecciones entre métodos ofrece un criterio práctico de priorización de casos, permitiendo focalizar los recursos de las unidades de riesgo y cumplimiento en aquellos eventos donde existe mayor consenso algorítmico sobre su carácter anómalo.

En conjunto, estos elementos sugieren que la integración de técnicas de aprendizaje automático en la arquitectura de monitoreo puede contribuir a fortalecer la resiliencia operativa de las entidades financieras y su capacidad de respuesta ante eventos de pérdida.

9. Recomendaciones

- Extender el análisis incorporando variables adicionales relacionadas con el canal de la transacción, el tipo de comercio, la frecuencia de uso y la localización geográfica, con el fin de capturar patrones más ricos y alineados con las tipologías de riesgo identificadas por las autoridades supervisoras.
- Implementar un esquema de recalibración periódica de los modelos, de manera que los parámetros y umbrales se ajusten a cambios en el comportamiento de los clientes, en las condiciones de mercado o en la estrategia de negocio.
- Integrar los resultados en una plataforma de monitoreo continuo que permita generar alertas con distintos niveles de severidad, conectadas con flujos de trabajo para la revisión manual y el registro de decisiones, de acuerdo con las mejores prácticas de gestión integral de riesgos [29, 31, 6].

10. Limitaciones

- El conjunto de datos utilizado tiene carácter sintético y se emplea con fines ilustrativos, por lo que sus resultados no deben interpretarse como reflejo directo de la realidad operativa de una entidad específica.
- La ausencia de etiquetas de fraude o de eventos de pérdida asociados impide calcular medidas clásicas de desempeño (como precisión, sensibilidad o valor económico esperado), limitando la evaluación a un análisis descriptivo y exploratorio.
- El umbral de aproximadamente un 5 % de anomalías se definió de forma heurística para este estudio. En un entorno real, dicho parámetro debería fijarse a partir de criterios de apetito de riesgo, capacidad operativa de análisis de alertas y experiencia histórica de cada institución.

Bibliografía

[1] C. C. Aggarwal. *Outlier Analysis*. 2nd. Cham: Springer, 2017. DOI: 10.1007/978-3-319-47578-3.

[2] E. I. Altman. "Financial Ratios, Discriminant Analysis and the Prediction of Corporate Bankruptcy". En: *The Journal of Finance* 23.4 (1968), págs. 589-609. DOI: 10.1111/j.1540-6261.1968.tb00843.x.

[3] J. An y S. Cho. *Variational Autoencoder based Anomaly Detection using Reconstruction Probability*. arXiv preprint arXiv:1512.09300. 2015.

[4] Asamblea Legislativa de Costa Rica. *Ley N. 8204: Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo (texto consolidado)*. Sistema Costarricense de Información Jurídica (SCIJ). 2001. URL: https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=48392&nValor3=93996&param1=NRTC&strTipM=TC.

[5] J. O. Awoyemi, A. O. Adetunmbi y S. A. Oluwadare. "Credit Card Fraud Detection Using Machine Learning Techniques: A Comparative Analysis". En: *2017 International Conference on Computing Networking and Informatics (ICCNI)*. IEEE, 2017, págs. 1-9. DOI: 10.1109/ICCNI.2017.8123782.

[6] Bank for International Settlements. *Machine Learning Approaches to Anomaly Detection in High-Value Payment Systems*. Inf. téc. 1188. BIS Working Papers, 2025. URL: https://www.bis.org/publ/work1188.pdf.

[7] V. Barnett y T. Lewis. *Outliers in Statistical Data*. 3rd. Chichester: Wiley, 1994.

[8] M. R. Berthold y F. Höppner. *On Clustering Time Series Using Euclidean Distance and Pearson Correlation*. arXiv preprint arXiv:1601.02213. 2016. URL: https://arxiv.org/abs/1601.02213.

[9] L. Breiman. "Random Forests". En: *Machine Learning* 45.1 (2001), págs. 5-32. DOI: 10.1023/A:1010933404324.

[10] L. Breiman. "Random Forests". En: *Machine Learning* 45.1 (2001), págs. 5-32. DOI: 10.1023/A:1010933404324. URL: https://doi.org/10.1023/A:1010933404324.

[11] J. A. Caldwell, P. J. Niro, E. K. Farina, J. P. McClung, G. R. Caron y H. R. Lieberman. "A Z-score based method for comparing the relative sensitivity of behavioral and physiological metrics including cognitive performance, mood, and hormone levels". En: *PLOS ONE* 14.8 (2019), e0220749. DOI: 10.1371/journal.pone.0220749.

[12] R. Chalapathy y S. Chawla. *Deep Learning for Anomaly Detection: A Survey*. arXiv preprint arXiv:1901.03407. 2019.

[13] V. Chandola, A. Banerjee y V. Kumar. "Anomaly Detection: A Survey". En: *ACM Computing Surveys* 41.3 (2009), págs. 1-58. DOI: 10.1145/1541880.1541882.

[14] DataDrivenInvestor. *Anomaly Detection with Z-Score: Pick the Low Hanging Fruits*. Online article. 2019. URL: https://www.datadriveninvestor.com/2019/11/27/anomaly-detection-with-z-score-pick-the-low-hanging-fruits/.

[15] T. Hastie, R. Tibshirani y J. Friedman. *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*. 2nd. New York: Springer, 2009. DOI: 10.1007/978-0-387-84858-7.

[16] A. Herreros-Martínez, R. Magdalena-Benedicto, J. Vila-Francés, A. Serrano-López y S. Pérez-Díaz. "Applied Machine Learning to Anomaly Detection in Enterprise Purchase Processes". En: *arXiv preprint arXiv:2405.14754* (2024). URL: https://arxiv.org/abs/2405.14754.

[17] G. E. Hinton y R. R. Salakhutdinov. "Reducing the Dimensionality of Data with Neural Networks". En: *Science* 313.5786 (2006), págs. 504-507. DOI: 10.1126/science.1127647. URL: https://www.science.org/doi/10.1126/science.1127647.

[18] T. K. Ho. "The Random Subspace Method for Constructing Decision Forests". En: *IEEE Transactions on Pattern Analysis and Machine Intelligence*. Vol. 20. 8. IEEE, 1998, págs. 832-844. DOI: 10.1109/34.709601.

[19] B. Iglewicz y D. C. Hoaglin. *How to Detect and Handle Outliers*. Milwaukee, WI: ASQ Quality Press, 1993.

[20] V. Khorasani. *Bank Transaction Dataset for Fraud Detection*. https://www.kaggle.com/datasets/valakhorasani/bank-transaction-dataset-for-fraud-detection. Dataset. 2024. (Visitado 09-11-2025).

[21] X. Li, D. Tripe y C. Malone. *Measuring Bank Risk: An Exploration of Z-Score*. Working paper / EFMA Symposium; also available on SSRN. 2017. URL: https://www.efmaefm.org/0EFMSYMPOSIUM/2017/papers/Measuring%20Bank%20Risk_An%20exploration%20of%20z-score.pdf.

[22] F. T. Liu, K. M. Ting y Z.-H. Zhou. "Isolation Forest". En: *Proceedings of the 2008 IEEE International Conference on Data Mining (ICDM)*. 2008, págs. 413-422. DOI: 10.1109/ICDM.2008.17.

[23] F. T. Liu, K. M. Ting y Z.-H. Zhou. "Isolation-Based Anomaly Detection". En: *Proceedings of the 8th IEEE International Conference on Data Mining (ICDM)*. IEEE, 2008, págs. 413-422. DOI: 10.1109/ICDM.2008.17. URL: https://doi.org/10.1109/ICDM.2008.17.

[24] F. T. Liu, K. M. Ting y Z.-H. Zhou. "Isolation-Based Anomaly Detection". En: *ACM Transactions on Knowledge Discovery from Data* 6.1 (2012), 3:1-3:39. DOI: 10.1145/2133360.2133363.

[25] J. Patel y otros. "Leveraging K-Means Clustering and Z-Score for Anomaly Detection". En: *Journal of Big Data Analytics* 12.2 (2025), pág. 43. DOI: ....

[26] A. Pumsirirat y L. Yan. "Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine". En: *International Journal of Advanced Computer Science and Applications (IJACSA)* 9.1 (2018), págs. 18-25. URL: https://thesai.org/Publications/ViewPaper?Volume=9&Issue=1&Code=IJACSA&SerialNo=3.

[27] L. Sabetti y R. Heijmans. "Shallow or deep? Training an autoencoder to detect anomalous flows in a retail payment system". En: *Latin American Journal of Central Banking* 2.2 (2021), pág. 100031. DOI: 10.1016/j.lajcb.2021.100031. URL: https://www.sciencedirect.com/science/article/pii/S2666143821000119.

[28] M. Sakurada y T. Yairi. "Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction". En: *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. 2014, págs. 1137-1142. DOI: 10.1109/SMC.2014.6974417.

[29] Superintendencia General de Entidades Financieras (SUGEF). *Acuerdo SUGEF 1-05: Gestión integral de riesgos*. https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=56045&nValor3=116789&strTipM=

TC. Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), Costa Rica. 2005.

[30] Superintendencia General de Entidades Financieras (SUGEF). *Reglamento para la prevención del riesgo de LC/FT/FPADM (Acuerdo SUGEF 13-19), versión vigente*. Inf. téc. Versión v6, 24 de mayo de 2024. CONASSIF / SUGEF, 2024. URL: https://www.sugef.fi.cr/normativa/normativa_vigente/SUGEF%2013-19%20%28v6%2024%20de%20mayo%202024%29.pdf.

[31] C. de Supervisión Bancaria de Basilea. *Principios para la gestión eficaz del riesgo operacional*. https://www.bis.org/publ/bcbs189.pdf. Banco de Pagos Internacionales (BIS), Basilea. 2011.

[32] V. Vijayakumar, N. S. Divya, P. Sarojini y K. Sonika. "Isolation Forest and Local Outlier Factor for Credit Card Fraud Detection System". En: *International Journal of Engineering and Advanced Technology (IJEAT)* 9.4 (2020). Available at SSRN: 3925017, págs. 261-265. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3925017.

[33] R. Yahiaoui, M. A. Chikh y A. Ghomari. "Fraud Detection in Banking Transactions Using Random Forest Classifier". En: *International Journal of Advanced Computer Science and Applications (IJACSA)* 13.5 (2022), págs. 150-158. DOI: 10.14569/IJACSA.2022.0130518. URL: https://thesai.org/Publications/ViewPaper?Volume=13&Issue=5&Code=IJACSA&SerialNo=18.

[34] W. Zhang, L. Chen e Y. Sun. "Anomaly Detection on Blockchain Transactions Using Isolation Forest and Graph-Based Models". En: *Proceedings of the International Conference on Machine Learning Applications*. SCITEPRESS, 2025, págs. 102-113. URL: https://www.scitepress.org/publishedPapers/2025/134416/pdf/index.html.

[35] C. Zhou y R. C. Paffenroth. "Anomaly Detection with Robust Deep Autoencoders". En: *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*. ACM, 2017, págs. 665-674. DOI: 10.1145/3097983.3098052. URL: https://dl.acm.org/doi/10.1145/3097983.3098052.

[36] B. Zong, Q. Song, M. Min, W. Cheng, C. Lumezanu, D. Cho y H. Chen. "Deep Autoencoding Gaussian Mixture Model for Unsupervised Anomaly Detection". En: *Proceedings of the International Conference on Learning Representations (ICLR) Workshop*. 2018.

Anexos

A. Descripción de la aplicación

Se desarrolló una aplicación en `Shiny`, la cual funciona como un sistema interactivo de detección de anomalías. Al abrir la interfaz, el usuario observa una pantalla dividida en dos secciones principales. En el panel izquierdo se encuentra un conjunto de valores numéricos que permiten ingresar las características de una transacción específica: el monto de la transacción, el balance de la cuenta, la duración de la transacción en segundos, el número de intentos de inicio de sesión y la edad del cliente. Cada vez que el usuario modifica alguno de estos valores, la aplicación construye internamente un nuevo registro con dicha información y vuelve a evaluarlo automáticamente. Esta evaluación se realiza de manera simultánea mediante los tres métodos descritos para la detección de anomalías, cuyos resultados se muestran en el panel derecho de la interfaz, organizado a través de tres pestañas: *Z-Score*, *Isolation Forest* y *Autoencoder*. Cada pestaña proporciona una clasificación independiente sobre si la transacción introducida debe considerarse como consistente o como potencialmente atípica.

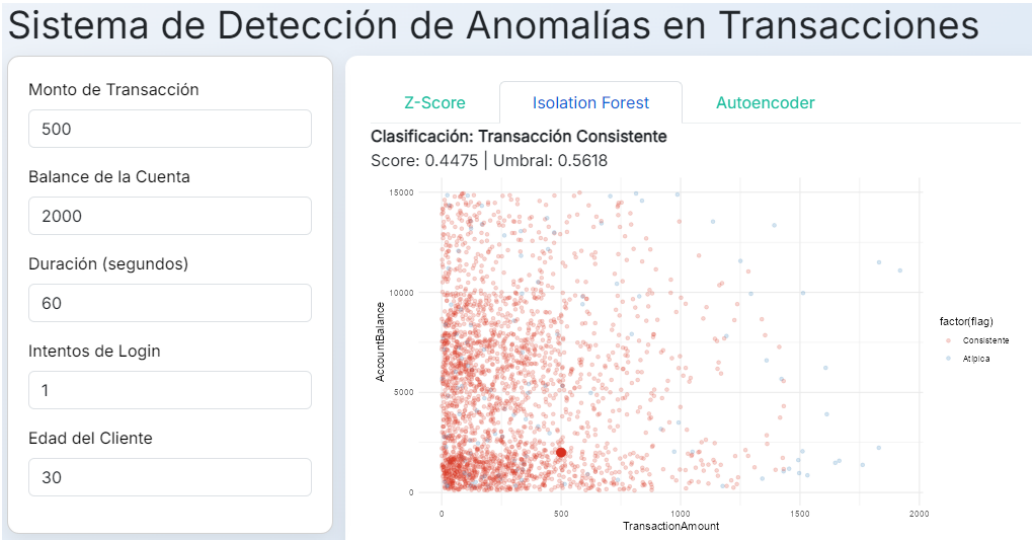

Figura 7: Interfaz para detección de anomalías en transacciones.

Fuente: Elaboración propia.

En la pestaña *Z-Score* se implementa el método más sencillo de los tres. Antes de iniciar la aplicación, se calcula la media y la desviación estándar del monto de transacción a partir del conjunto de datos históricos. Con estos valores se define un umbral estadístico de referencia igual a la media más dos desviaciones estándar. El criterio de decisión es directo: si el monto de la transacción ingresada por el usuario supera dicho umbral, la operación se clasifica como una *transacción atípica*; en caso contrario, se considera *transacción consistente*. Además, se presenta un

gráfico en el plano `TransactionAmount` (eje horizontal) frente a `AccountBalance` (eje vertical), donde se representan todas las transacciones históricas coloreadas según su clasificación con este método. La transacción que ha introducido el usuario aparece destacada como un punto de mayor tamaño y coloreado de acuerdo con su categoría, lo que permite visualizar su posición relativa dentro del conjunto de datos.

La pestaña *Isolation Forest* muestra la evaluación de la transacción considerando simultáneamente todas las características ingresadas en el panel izquierdo: el monto, el balance de la cuenta, la duración de la operación, los intentos de inicio de sesión y la edad del cliente. A partir del comportamiento histórico de miles de transacciones, el sistema asigna a cada operación un puntaje que indica qué tan inusual resulta en comparación con el resto. Con base en estos puntajes se define un umbral que separa las transacciones consideradas normales de aquellas que presentan un comportamiento atípico. Si el puntaje de la transacción ingresada supera dicho umbral, el sistema la clasifica como atípica; de lo contrario, la considera consistente. En la interfaz se muestra la clasificación obtenida, el puntaje específico de la transacción y el valor del umbral de referencia. Además, se presenta un gráfico donde se visualizan las transacciones históricas junto con la operación evaluada, permitiendo apreciar su posición relativa dentro del conjunto de datos.

La pestaña *Autoencoder* evalúa la transacción comparándola con los patrones habituales aprendidos a partir del historial completo de operaciones. Este método analiza simultáneamente todas las características ingresadas en el panel izquierdo y determina qué tan bien encaja la transacción dentro del comportamiento normal observado en los datos. Para ello, el sistema calcula un valor de error que refleja la diferencia entre la transacción analizada y los patrones que el modelo considera típicos. A partir del historial de errores se establece un umbral que permite distinguir las operaciones coherentes de las que presentan comportamientos inusuales. Si el error asociado a la transacción supera ese umbral, el sistema la clasifica como atípica; si se encuentra por debajo, se considera consistente. En la interfaz se muestran la clasificación obtenida, el valor exacto del error y el umbral utilizado. Además, se presenta un gráfico donde se visualizan las transacciones históricas y la transacción evaluada, lo que permite visualizar el comportamiento dentro del conjunto.

B. Repositorio del proyecto

El código fuente del proyecto se encuentra disponible en el siguiente enlace:

Enlace a repositorio en GitHub