Modelo analítico basado en aprendizaje automático para la detección de transacciones anómalas en la gestión del riesgo financiero

Gustavo Amador, Luis Amey, Johan Castaño,
Javier Hernández, Anthony Jiménez

Riesgo en Instituciones Financieras I
Universidad de Costa Rica

28 de noviembre de 2025

Contenido

Riesgo operativo en entidades financieras

- El **riesgo operativo** se asocia a pérdidas derivadas de:
  - Fallas en procesos internos,
  - Errores humanos,
  - Fallas en sistemas,
  - Eventos externos.
- En 2012, HSBC fue multado con miles de millones por fallas en controles contra lavado de dinero.
- Las transacciones son un punto crítico donde estos riesgos se materializan.
- La analítica de datos y los métodos de detección de anomalías pueden:
  - Apoyar el monitoreo continuo,
  - Priorizar casos para revisión,
  - Reducir la probabilidad de incidentes no detectados.

Motivación del estudio

- Explorar el uso de **métodos no supervisados** para detectar transacciones inusuales.
- Aprovechar información transaccional histórica para:
  - Identificar patrones normales de comportamiento,
  - Marcar posibles desviaciones relevantes.
- Integrar estos hallazgos como una herramienta complementaria dentro de la gestión del riesgo operativo.

Objetivo general

Desarrollar y comparar modelos de detección de transacciones anómalas como herramienta complementaria para la gestión del riesgo operativo en una entidad financiera.

Objetivos específicos

- Aplicar distintos métodos de detección de anomalías:
  - Estadístico (Z-score),
  - Basado en árboles (Isolation Forest),
  - Basado en redes neuronales (Autoencoder).
- Analizar el comportamiento de las anomalías en función de variables financieras relevantes.
- Evaluar el solapamiento entre los modelos y discutir su utilidad práctica para monitoreo de riesgo operativo.

Descripción de los datos

- Base de datos de transacciones bancarias simuladas.
- **2 512** transacciones y **16** variables.
- Sin valores faltantes.
- Variables clave:
  - Monto de la transacción (Transaction Amount),
  - Saldo en cuenta (Account Balance),
  - Fecha de la transacción,
  - Duración de la transacción,
  - Intentos de inicio de sesión,
  - Canal y ubicación,
  - Ocupación y dispositivo de transacción, entre otras.

Resumen estadístico de variables numéricas

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.

- Montos y saldos con alta dispersión y presencia de valores extremos.
- Patrones estables en duración e intentos de login.
- Población adulta y económicamente activa.
- La variabilidad del dataset justifica técnicas avanzadas de detección de anomalías.

Resumen estadístico de variables numéricas

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

Cuadro 2: Distribución por tipo de transacción.

- La mayoría de las operaciones son débitos, lo que indica un uso centrado en pagos o salidas de fondos.

Resumen estadístico de variables numéricas

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

Cuadro 3: Distribución por canal de transacción.

- Los tres canales tienen participaciones muy similares; no hay concentración en un único medio.

Resumen estadístico de variables numéricas

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

Cuadro 4: Distribución por ocupación del cliente.

- Distribución uniforme entre las ocupaciones.

Resumen estadístico de variables numéricas

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

Cuadro 5: Distribución horaria de las transacciones.

- Existe un pico operativo a las 16:00, lo que señala un horario de mayor carga transaccional.

Resumen estadístico de variables numéricas

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.

- Las transacciones están distribuidas de manera equilibrada entre distintas ciudades, sin una concentración marcada en un único punto geográfico.

Resumen estadístico de variables numéricas

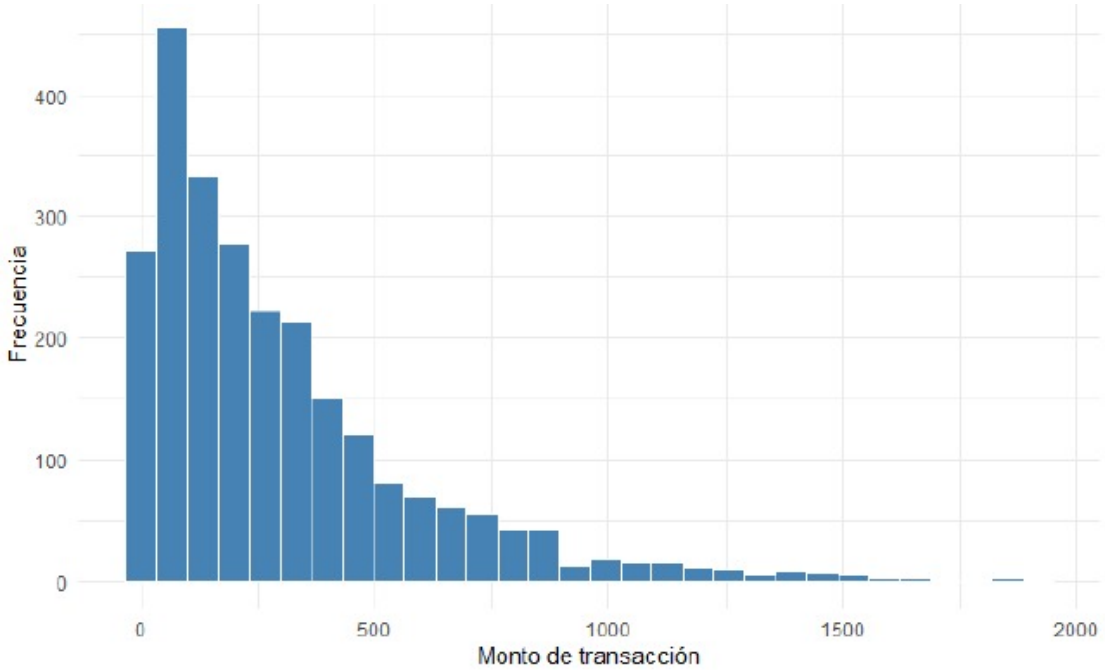


Figura 2: Histograma de las cantidades de transacciones.

- Las operaciones de bajo valor dominan.
- Las transacciones de gran cuantía, pueden representan puntos críticos para riesgo operativo y posibles anomalías.

Metodología general

- Se realiza una **exploración y limpieza** inicial para identificar valores faltantes, inconsistencias y posibles duplicados.
- Las variables numéricas se **estandarizan** para hacer comparables los distintos métodos.
- Se aplican tres técnicas no supervisadas de detección de anomalías:
  - **Z-score**: detección basada en desviaciones respecto a la media.
  - **Isolation Forest**: identifica puntos que son "fáciles de aislar".
  - **Autoencoder**: reconstrucción de patrones normales mediante una red neuronal.

Metodología general

- Se definen **umbrales** para clasificar observaciones como normales o anómalas.
- Se compara el desempeño de los modelos según:
  - **Porcentaje de anomalías** detectadas.
  - **Coincidencia** entre métodos.
  - **Distribución** de las anomalías según monto y saldo.

Método Z-score

- Para una variable numérica X, se define el Z-score como:

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

  donde μ es la media y σ la desviación estándar.
- Idea central:
  - Valores con $|z|$ muy grande son considerados **atípicos**.

Método Isolation Forest

- Algoritmo basado en **bosques de árboles aleatorios**.
- Construye múltiples árboles de partición del espacio de variables.
- Las observaciones que requieren **pocas divisiones** para ser aisladas son clasificadas como más anómalas.
- Proporciona un *score de anomalía* continuo, sobre el cual se fija un umbral.

Método Autoencoder

- Red neuronal diseñada para **reconstruir** la entrada.
- Arquitectura básica:
  - **Encoder**: comprime la información de la transacción en una representación de menor dimensión.
  - **Decoder**: intenta reconstruir la transacción original a partir de esa representación.
- Se entrena principalmente con transacciones que se consideran **normales**.
- El **error de reconstrucción** (por ejemplo, MSE) sirve como indicador:
  - Error bajo $\Rightarrow$ comportamiento normal,
  - Error alto $\Rightarrow$ posible anomalía.

Resumen cuantitativo de anomalías

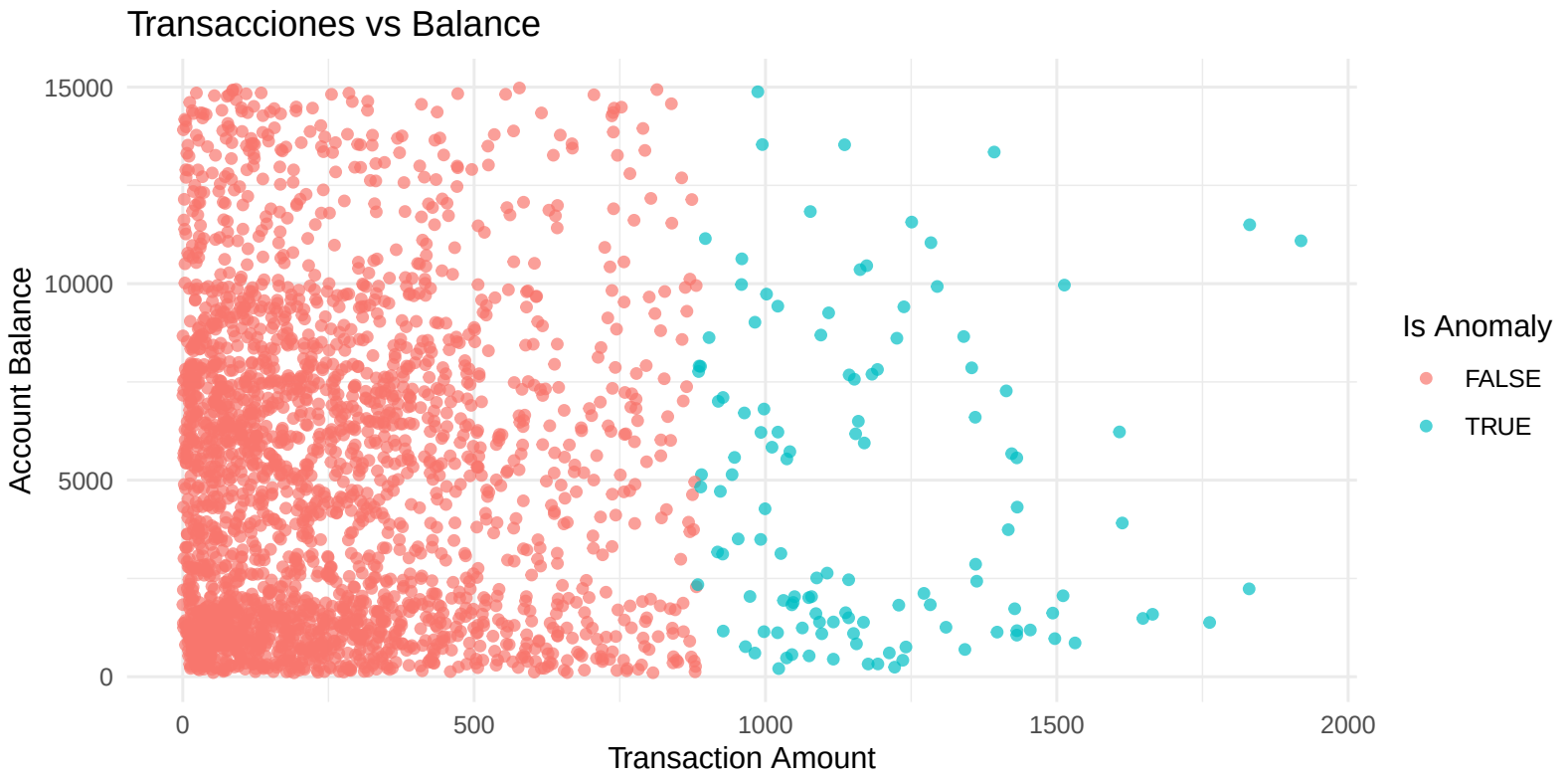
- Proporción de transacciones clasificadas como anómalas:

Modelo	% de anomalías
Z-score	$\approx 4{,}8\,\%$
Isolation Forest	$\approx 5{,}0\,\%$
Autoencoder	$\approx 5{,}0\,\%$

- Los tres métodos marcan una fracción relativamente pequeña de transacciones, coherente con la idea de que los eventos operativos relevantes son poco frecuentes.
- Correlación entre las clasificaciones de Autoencoder e Isolation Forest: $\approx 0{,}56$.
- Esto indica que capturan patrones parcialmente similares, pero no idénticos.

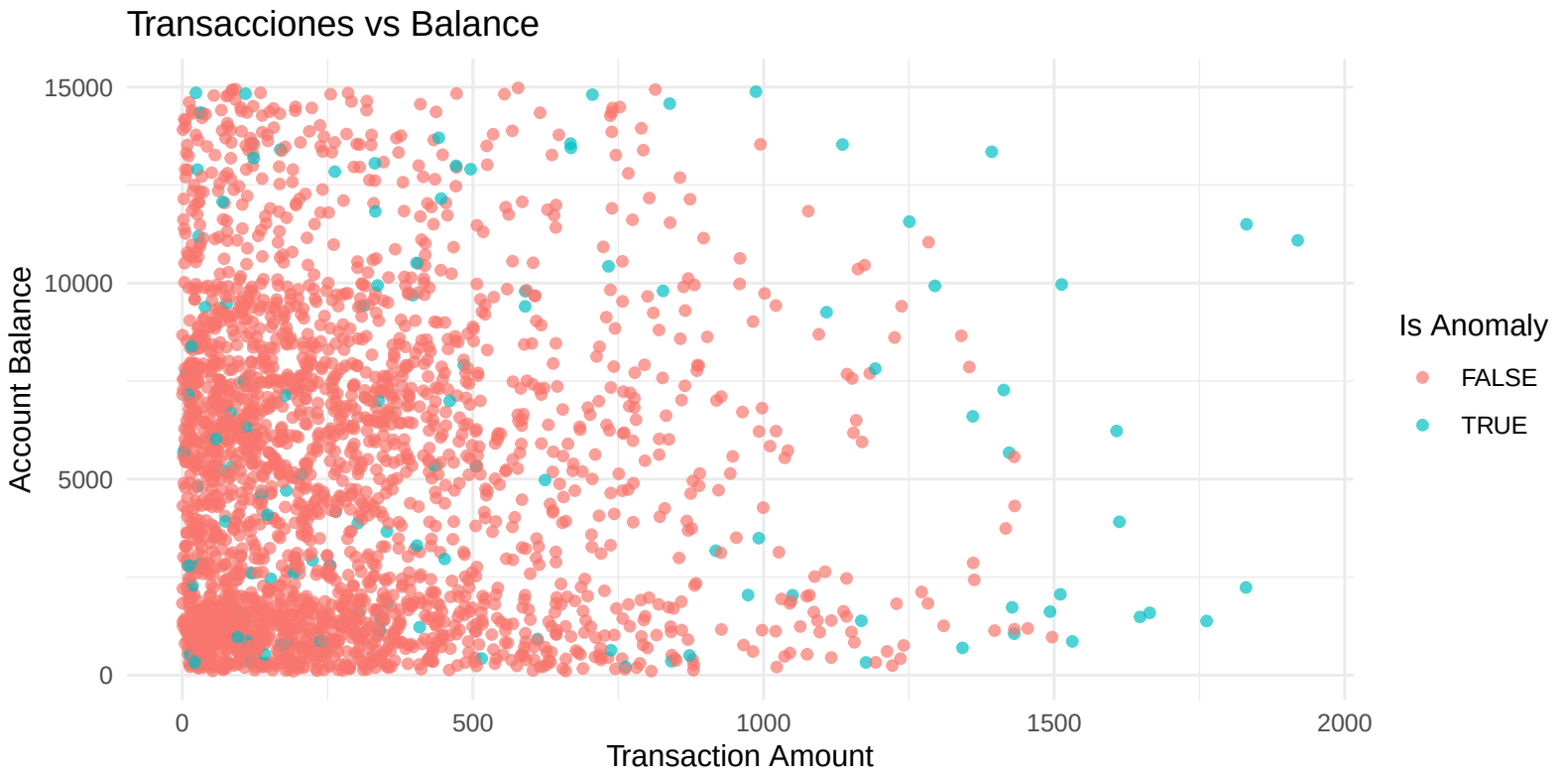
Resultados Z-score: Transacciones vs Saldo

- Los puntos marcados como anomalías corresponden a observaciones con valores extremos en una o más variables.
- Se observa que:
  - Clara separación entre nube de transacciones normales, y nube de transacciones inusuales.



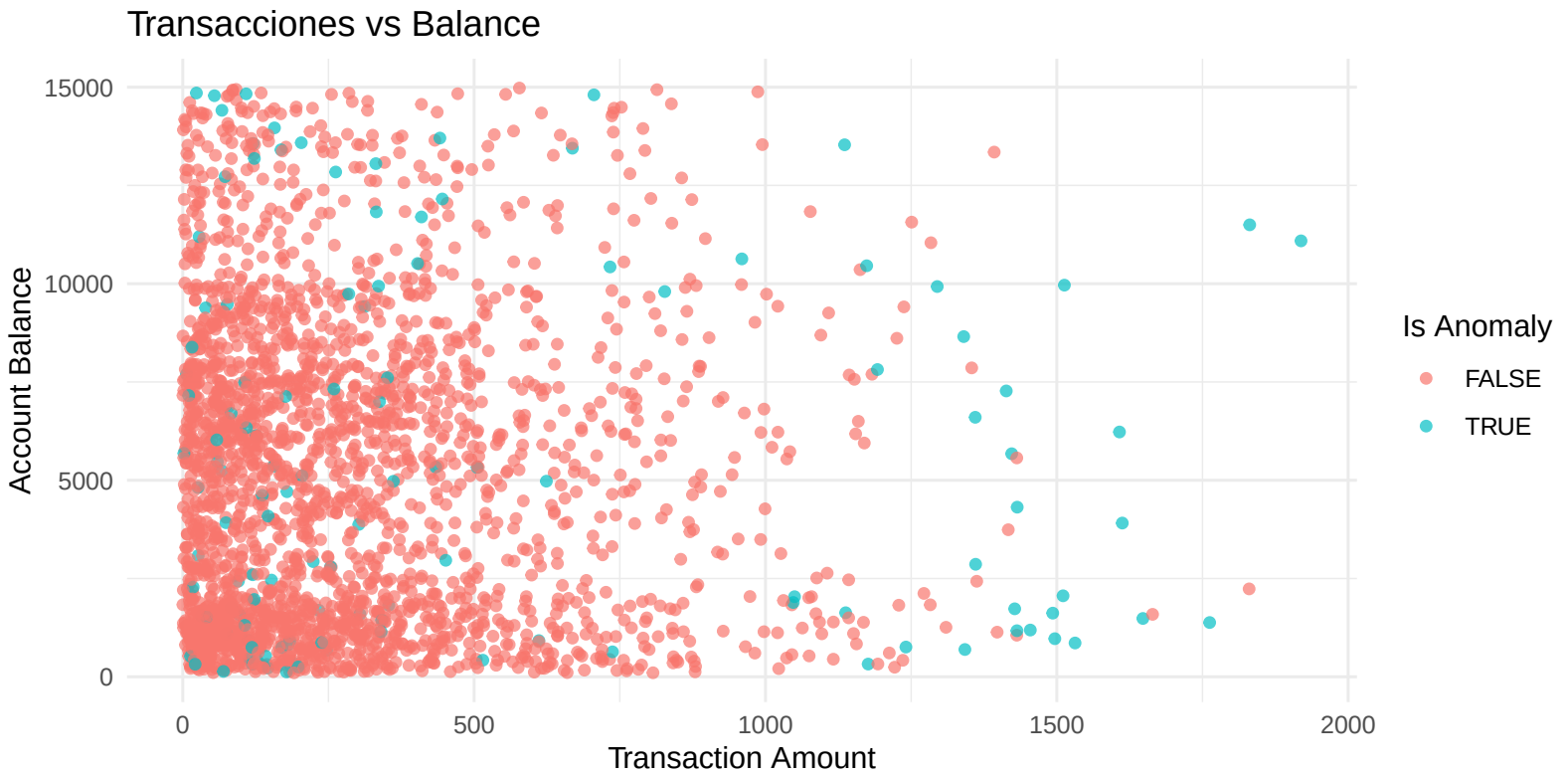
Resultados Isolation Forest: Transacciones vs Saldo

- Este modelo utiliza la estructura multivariante completa, no solo un indicador unidimensional.
- En el gráfico se aprecia que:
  - Algunas anomalías coinciden con las detectadas por Z-score,
  - Otras se ubican en regiones donde la densidad de puntos normales es baja, aún si no son extremas en un solo eje.



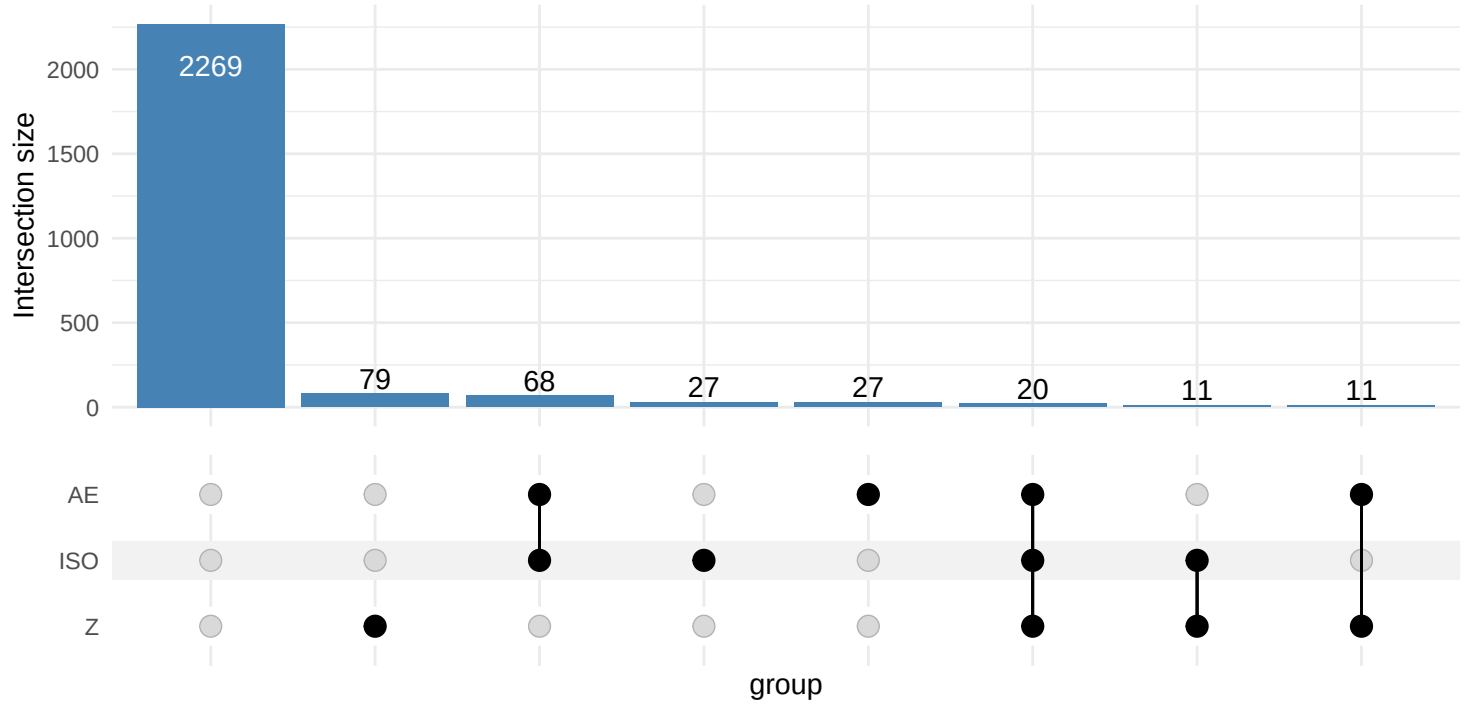
Resultados Autoencoder: Transacciones vs Saldo

- El modelo aprende un patrón de normalidad y marca como anómalas las observaciones que no logra reconstruir bien.
- En la figura se observa que:
  - Las anomalías se sitúan en zonas menos frecuentes del plano, coherentes con las regiones que el modelo considera atípicas.



Comparación entre modelos

- Intersección de transacciones marcadas como anómalas:



- Resultado clave:
  - Las transacciones en la intersección de los tres modelos son las candidatas más fuertes a **revisión prioritaria**,
  - Las detectadas por un solo modelo pueden corresponder a patrones específicos que solo ese enfoque está captando.

Interpretación en términos de riesgo operativo

- Las anomalías no se limitan a posibles fraudes:
  - Pueden reflejar errores de digitación,
  - Procesos mal configurados,
  - Operaciones fuera de parámetros establecidos.
- Los resultados obtenidos muestran que:
  - Es posible aislar un pequeño subconjunto de transacciones con comportamiento inusual,
  - Este subconjunto puede enfocarse para análisis detallado por parte de las áreas de riesgo y cumplimiento.
- Los modelos de anomalías funcionan como:
  - **Filtro inicial** en el monitoreo diario o semanal,
  - Herramienta de **priorización** para equipos de riesgo,
  - Apoyo para detectar patrones emergentes en el comportamiento transaccional.

Limitaciones y trabajo futuro

- Datos utilizados de carácter simulado o de ejemplo:
  - Falta evaluación con datos reales etiquetados (incidente/no incidente).
- Resultados sensibles a:
  - Elección de umbrales,
  - Selección de variables y transformaciones.
- Posibles extensiones:
  - Incorporar más variables de contexto (horario, geolocalización, historial largo),
  - Combinar estos métodos con reglas de negocio existentes,
  - Integrar esquemas supervisados cuando se disponga de etiquetas.

Conclusiones

- Los tres métodos detectan aproximadamente un **5 %** de transacciones como anómalas.
- El análisis visual muestra que estas anomalías se concentran en regiones poco densas del espacio de variables, coherente con el concepto de outlier.
- Existe un **solapamiento relevante** entre Isolation Forest y Autoencoder, apoyado por la correlación entre sus resultados.
- La combinación de:
  - Modelos estadísticos y de aprendizaje automático,
  - Visualizaciones sobre variables financieras clave,

  es una herramienta útil para la **gestión del riesgo operativo**.
- No reemplaza el juicio experto, pero:
  - Ayuda a priorizar casos,
  - Mejora la capacidad de detección temprana,
  - Complementa los controles tradicionales.

Preguntas