Análisis de Datos y BI - Proyecto de Detección de Fraudes

Creado por:

Jose Ibarra

Gabriela Lopez

Silvana Jaramillo

Análisis de Datos y BI - Proyecto de Detección de Fraudes - Riskova

Introducción

El proyecto consistió en el desarrollo de un **MVP (Producto Mínimo Viable)** para una plataforma de detección de fraudes en pagos electrónicos. Este MVP integró aprendizaje automático y análisis de datos para proporcionar una solución práctica y funcional.

El MVP incluye:

1. **Procesamiento de Datos:**
   Se realizó la carga y limpieza de datos transaccionales, abordando problemas como valores nulos, duplicados y escalado de características para garantizar que la información estuviera lista para su análisis.
2. **Modelo Predictivo:**
   Se entrenó e implementó un modelo de machine learning capaz de identificar transacciones sospechosas con precisión, evaluando su desempeño con métricas como precisión, recall y F1-score.
3. **Monitoreo en Tiempo Real:**
   Se desarrolló un sistema interactivo que permite visualizar transacciones en tiempo real, junto con alertas automáticas en caso de detectar posibles fraudes.

Descripción:

Desarrollaremos un modelo predictivo para detectar transacciones fraudulentas en una plataforma de pagos electrónicos, utilizando técnicas de aprendizaje automático y análisis de comportamiento.

Datos:

Dataset Sintético de Simulación (Fraud Detection de Kaggle):
https://www.kaggle.com/datasets/kartik2112/fraud-detection

Contexto: El Problema

- Más de 700.000 millones de transacciones con tarjetas de crédito al año
- Nilson Report: Pérdidas por fraude con tarjetas

de crédito en 2022 - 33.450 M USD

Fraude mundial con tarjetas de crédito

alcanzará los 43.000 M USD en 2026

Fuentes: privacy.com/blog/credit-card-fraud-statistics, www.merchantsavvy.co.uk/payment-fraud-statistics/

Riskova: Qué es?

- Sistema de detección y seguimiento de transacciones electrónicas fraudulentas
- Basado en técnicas de ciencia de datos y ML
- Input: Datos históricos de transacciones
- Output: Predicción de nuevas transacciones (legitima/fraude)

Riskova: Para quién?

- Entidades emisoras de tarjetas:
  - Bancos
  - Casas Comerciales
  - Fintechs
- Riesgo de actividad fraudulenta y pérdidas económicas
- Recursos destinados a la resolución de conflictos

Riskova: ¿Qué ofrece?

- Construcción de un modelo predictor de transacciones (fraude/no fraude) en tiempo real
- Diagnóstico a la fecha:

tipo de transacción, ubicación y tiempo

- Análisis estadístico avanzado de variables que

afectan la predicción

- Mejoramiento continuo de la herramienta oramiento continuo de la herramienta

Riskova: Potencial

- Herramienta confiable para prevenir actividad fraudulenta
- Ahorrar recursos destinados a compensaciones y resoluciones de conflictos
- Mejorar la percepción del producto y de

la empresa por parte de los consumidores

- Utilizar información entregada por los datos

para tomar medidas adicionales

1. Guías de Tableros Interactivos

1.1 Interpretación de los Gráficos

Los gráficos interactivos permiten explorar las relaciones entre diferentes variables, como las transacciones fraudulentas vs. legítimas. Se incluyen los siguientes tipos de gráficos:

- **Gráfico de torta**: Muestra la distribución de las transacciones, diferenciando entre transacciones fraudulentas y legítimas, para ofrecer una visión general del comportamiento del sistema.
- **Gráfico de matriz de confusión**: Representa la comparación entre las predicciones del modelo y los valores reales, facilitando la evaluación del rendimiento del modelo en términos de falsos positivos y falsos negativos.
- **Gráfico de caja (Boxplot)**: Se utiliza para analizar la relación entre el monto de las transacciones y su clasificación como fraude o no fraude, permitiendo identificar patrones en los valores atípicos.
- **Mapas geográficos**: Visualiza la distribución geográfica de las transacciones fraudulentas, ayudando a identificar las regiones con mayor actividad sospechosa y posibles focos de fraude.
- **Curvas ROC (Receiver Operating Characteristic)**: Permiten evaluar la capacidad del modelo para discriminar entre transacciones fraudulentas y no fraudulentas, visualizando el balance entre verdaderos positivos y falsos positivos.
- **Gráficos SHAP (SHapley Additive exPlanations)**: Ofrecen una interpretación detallada del modelo, mostrando la importancia de cada característica en la predicción de fraudes.

1.2 Uso de Filtros y Widgets

Los usuarios pueden interactuar con los datos utilizando los siguientes controles:

- **Filtros por Fecha**: Permiten visualizar los datos dentro de rangos temporales específicos.
- **Widgets para Ajustar Parámetros**: Los usuarios pueden seleccionar diferentes umbrales de fraude

1.3 Interactividad con Dashboards

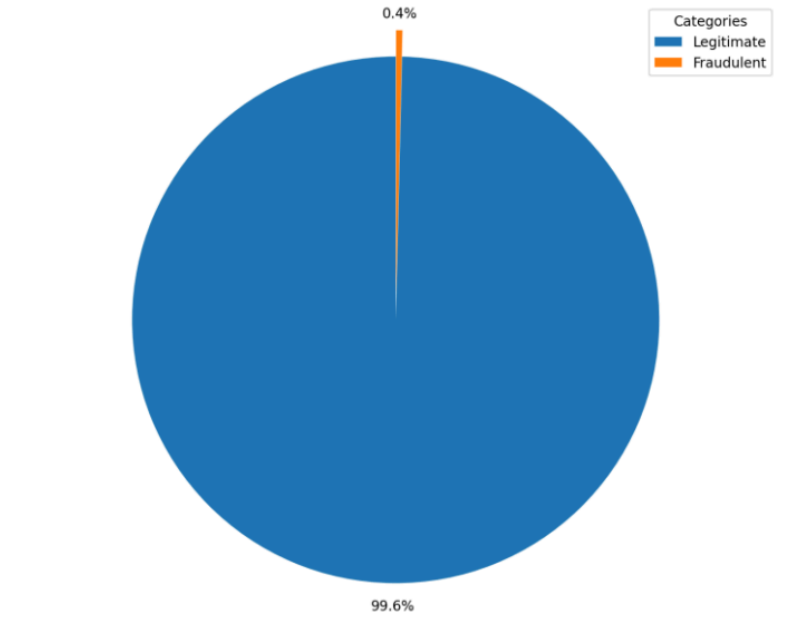
Se utilizó **Streamlit** para crear dashboards interactivos. Los usuarios pueden:

- **Visualizar métricas clave** como el porcentaje de fraudes detectados, número total de transacciones y tendencias temporales.
- **Aplicar filtros dinámicos** para segmentar los datos y realizar análisis a fondo.

Select Target Column for Analysis

Choose a column:

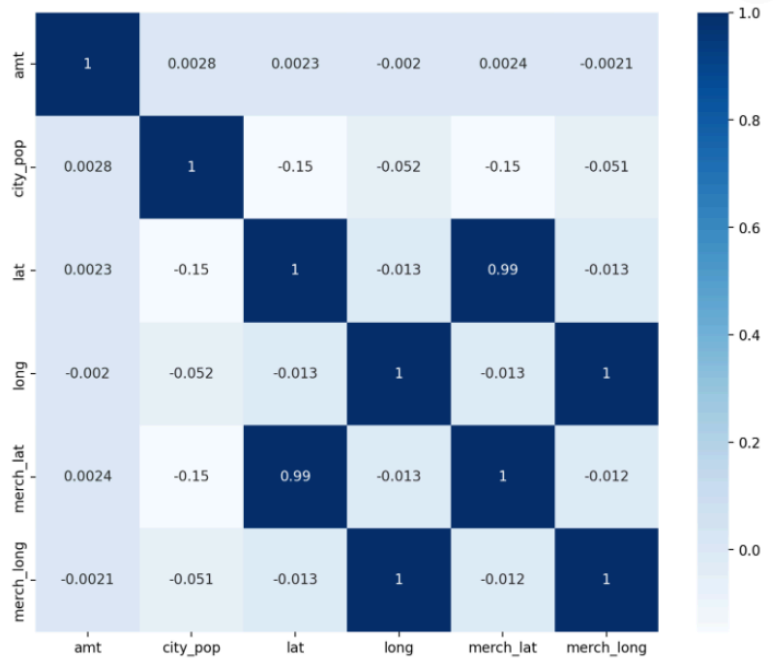
is_fraud



Correlation Matrix

Select columns for the correlation matrix:

amt × city_pop × lat × long × merch_lat × merch_long ×



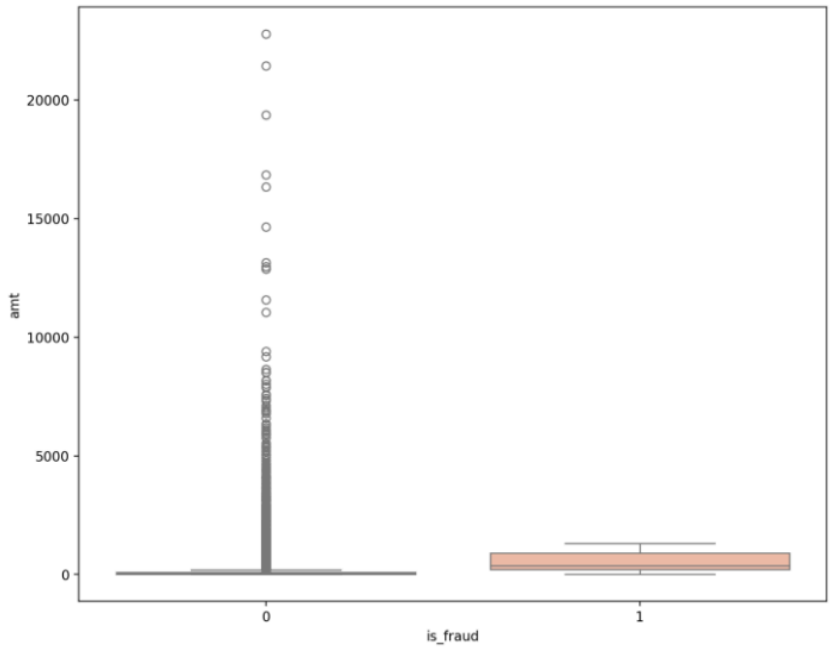
Fraud vs Non-Fraud Amount Distribution

Select X-axis column (categorical):

is_fraud

Select Y-axis column (numerical):

amt



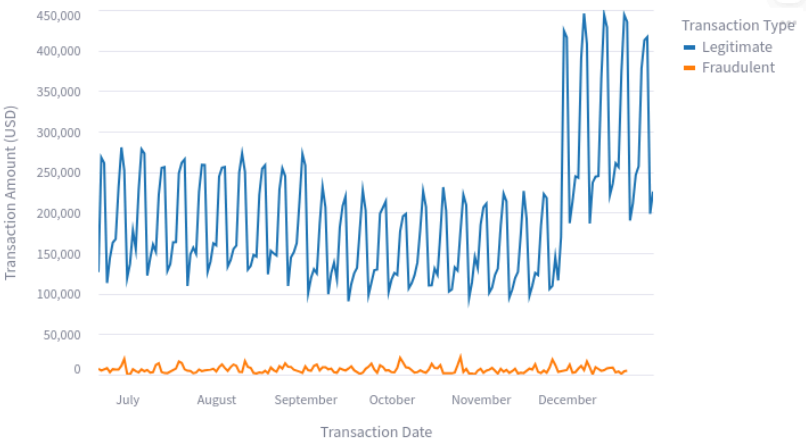
BI Dashboard

2020

2020 Summary

Total transactions	Legitimate	Fraudulent	Fraud/legit ratio (n)
555,719	553,574	2,145	0.39%

Total amount	Legit. Amount	Fraud. Aumount	Fraud/legit ratio ($)
$38,563k	$37,430k	$1,133k	3.03%



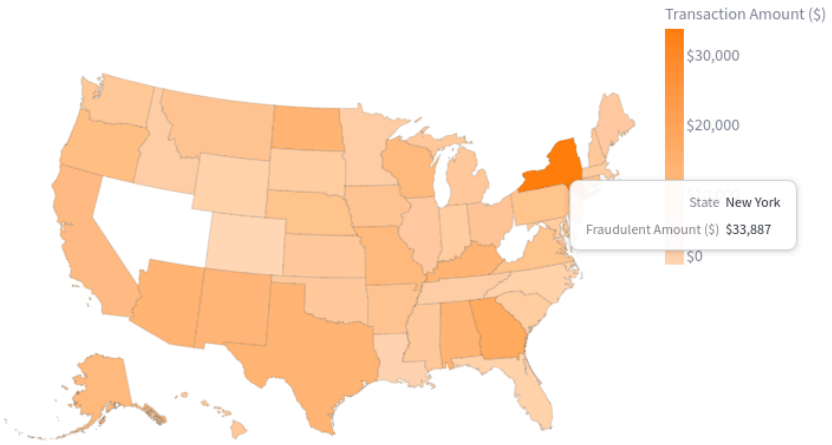
Select a month

All

Select Transaction Type

Fraudulent

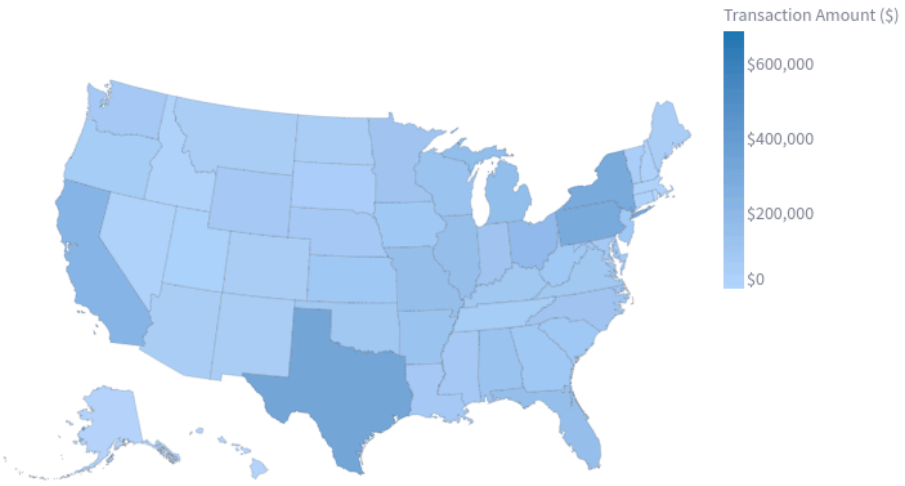
Fraudulent transactions by state - Year: 2020 | Month: All



Select Transaction Type

Legitimate

Legitimate transactions by state - Year: 2020 | Month: All



Select a state

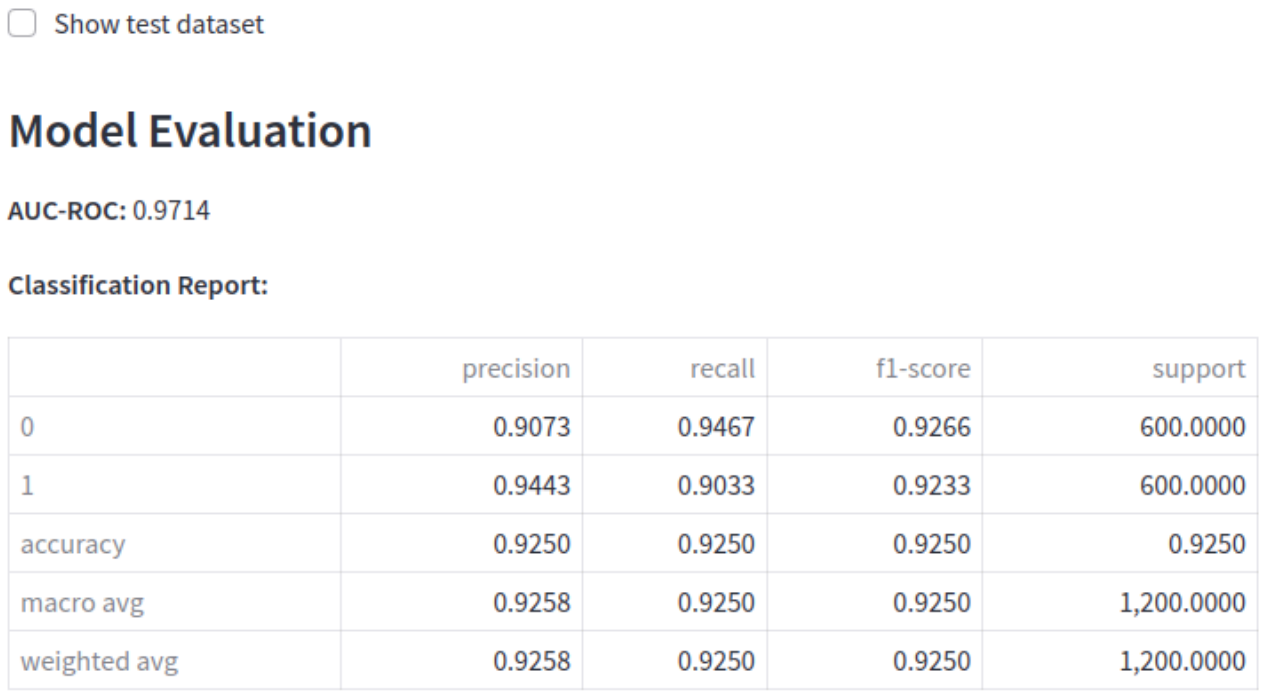
2. Descripción de KPIs

2.1 Porcentaje de Fraudes Detectados

- **Definición**: El porcentaje de transacciones fraudulentas detectadas por el modelo sobre el total de transacciones procesadas.
- **Objetivo**: Medir la efectividad del modelo para identificar fraudes.
- **Formula:**

$$\text{Porcentaje de Fraudes Detectados} = \frac{\text{Número de Fraudes Detectados}}{\text{Número Total de Transacciones}} \times 100$$

- **Interpretación**: El modelo mostró una precisión del 90% en la predicción de transacciones no fraudulentas y del 94% en la predicción de transacciones fraudulentas, lo cual es una excelente métrica, ya que prioriza la seguridad de la aplicación.


Show test dataset

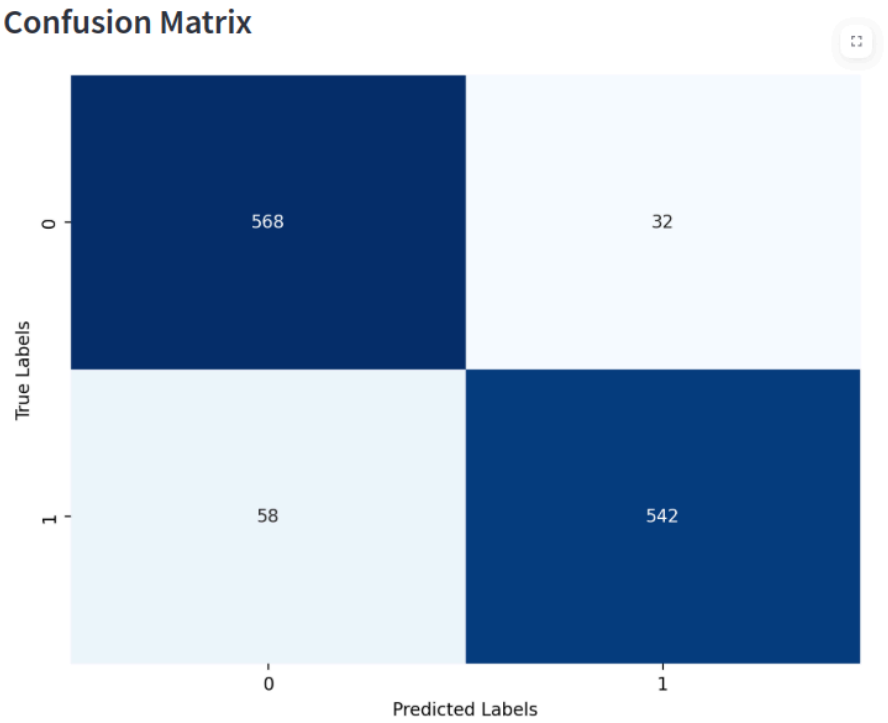
Model Evaluation

AUC-ROC: 0.9714

Classification Report:

	precision	recall	f1-score	support
0	0.9073	0.9467	0.9266	600.0000
1	0.9443	0.9033	0.9233	600.0000
accuracy	0.9250	0.9250	0.9250	0.9250
macro avg	0.9258	0.9250	0.9250	1,200.0000
weighted avg	0.9258	0.9250	0.9250	1,200.0000

- **Gráfico de matriz de confusión**: En cuanto a las predicciones legítimas, el modelo acertó en 568 de 600 casos, con 32 predicciones erróneas. Por el lado de las transacciones fraudulentas, el modelo detectó correctamente 542 transacciones fraudulentas verdaderas, mientras que 58 transacciones fraudulentas fueron clasificadas erróneamente como legítimas.



2.2 Tendencias Temporales de Fraude

- **Definición**: Este KPI mide la frecuencia de fraudes en diferentes periodos de tiempo (día, mes, hora).
- **Fórmula**:

$$\text{Tendencia Temporal de Fraude} = \frac{\text{Número de Fraudes en un Periodo}}{\text{Número de Transacciones en ese Periodo}} \times 100$$

- **Objetivo**: Identificar patrones de fraude y los momentos de mayor incidencia.
- **Interpretación**: Detectar picos de fraude que podrían estar relacionados con estacionalidades o eventos específicos.

3. Estrategias de Análisis de Datos

3.1 Preprocesamiento de Datos

El preprocesamiento de datos fue una de las fases clave para garantizar la calidad de los datos y la eficacia del modelo predictivo. Los pasos de preprocesamiento incluidos son:

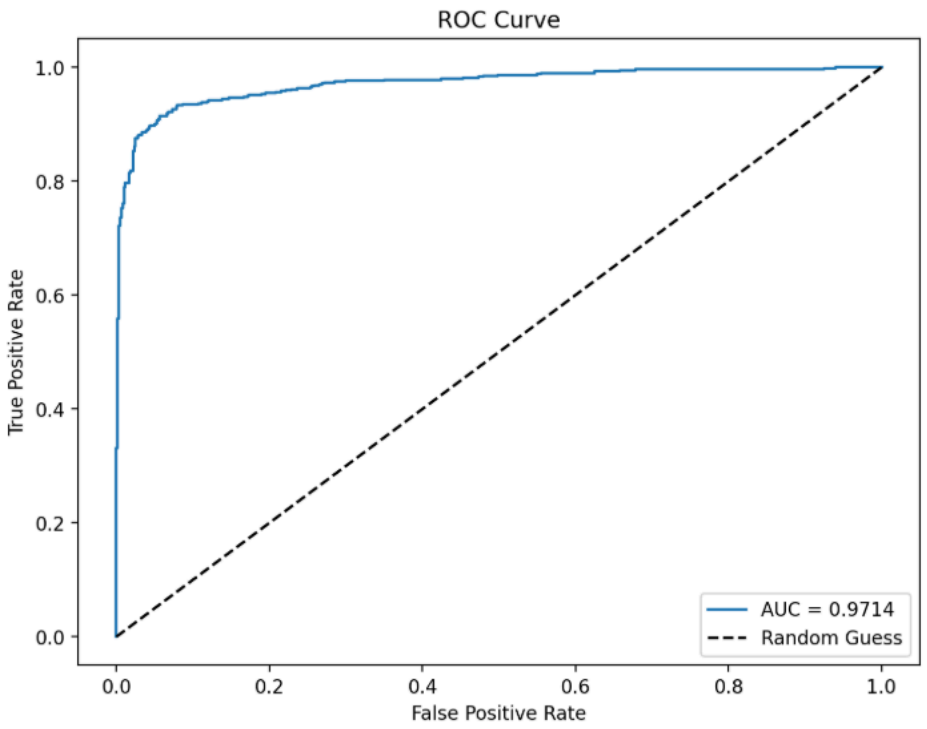
- **Carga de Datos**: Se utilizó pandas para cargar los archivos CSV que contenían las transacciones.
- **Limpieza de Datos**:
    - **Manejo de Valores Nulos**: Se remplazaron valores nulos con valores promedio o se eliminaron las filas con datos faltantes.

    - **Eliminación de Duplicados**: Se verificaron y eliminaron registros duplicados.
- **Transformaciones**:
    - **Cambio de tipo de dato**: Se modificó el tipo de dato de varias columnas para asegurar una correcta interpretación y procesamiento de la información. Este ajuste fue necesario para garantizar que los datos fueran adecuados para el análisis y el entrenamiento del modelo.

3.2 Modelado Predictivo

- **Entrenamiento del Modelo**: Se utilizó un modelo de Redes Neuronales Artificiales (RNA) para detectar fraudes.
- **Evaluación del Modelo**: Se utilizaron métricas como la **precisión**, **recall** y **F1-score** para evaluar el desempeño del modelo.
- **Curvas ROC**: Se generó la curva ROC para visualizar el rendimiento del modelo y ajustar el umbral de decisión.

ROC Curve

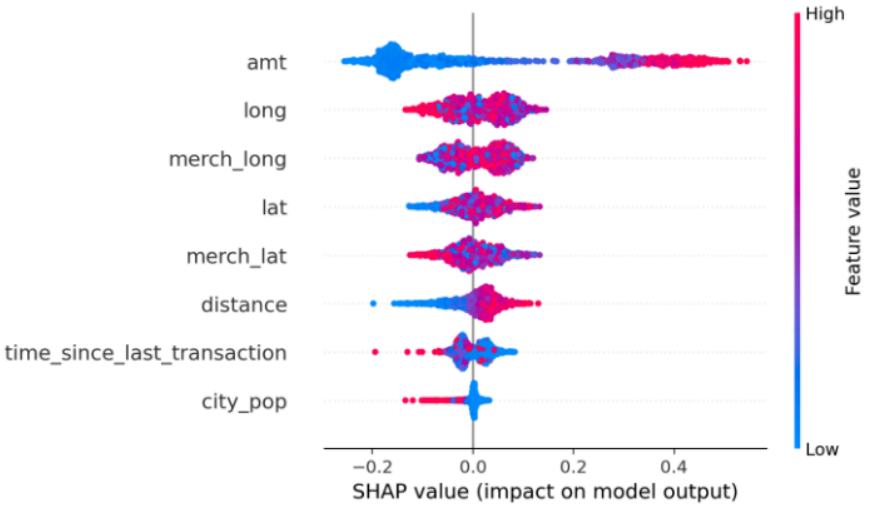


4.3 Visualización de los Resultados

- **Gráficos de Importancia de Características**: Utilizando técnicas como el análisis de características, se visualizó qué variables eran más influyentes para detectar fraudes.
- **SHAP Values**: En los gráficos de SHAP se identificó que el monto tiene un impacto significativo en la predicción del modelo. Además, en el gráfico de dependencia de SHAP se observó que tanto el monto como la distancia son las características más influyentes en las predicciones del modelo.

Model Interpretation with SHAP

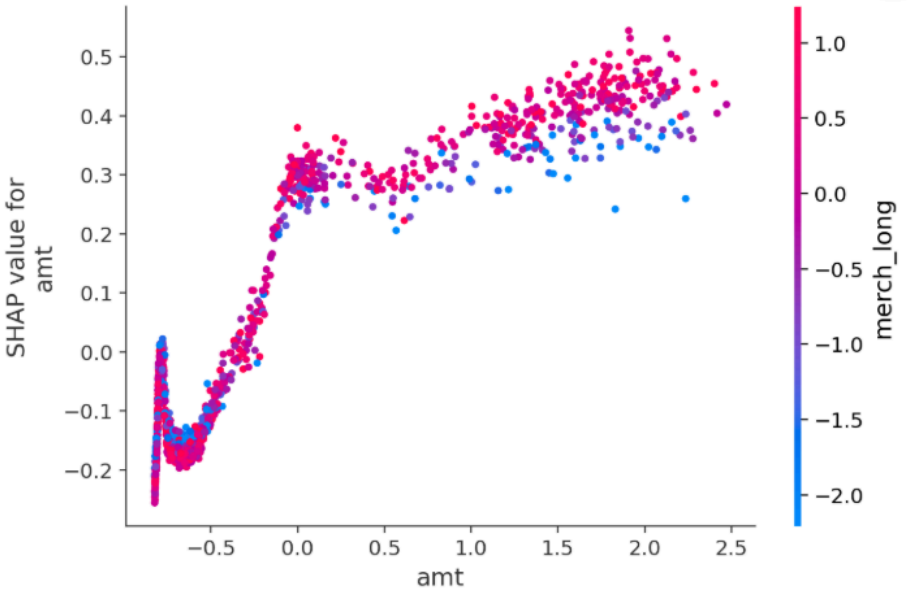
SHAP Summary Plot

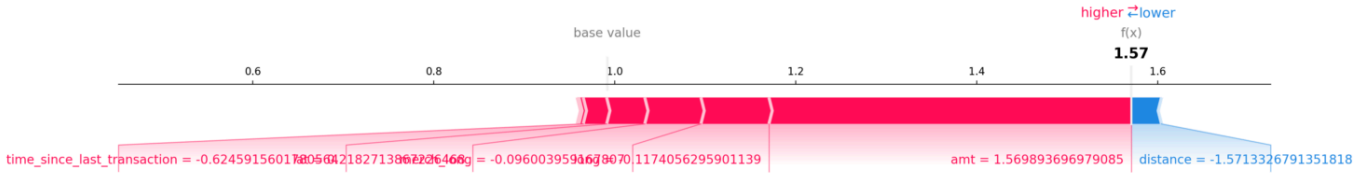


SHAP Dependence Plot

Select a feature for dependence plot:

amt





5. Conclusiones y Resultados

Impacto del Modelo

El modelo de predicción desarrollado logró identificar las transacciones fraudulentas con una alta precisión. Además, la visualización en tiempo real permitió a los usuarios monitorear las transacciones y generar alertas automáticas en caso de detectar fraude.

Mejoras Futuras

- **Optimización de Hiperparámetros**: Se explorarán diferentes combinaciones de hiperparámetros para mejorar el rendimiento del modelo.
- **Integración de Datos Externos**: Se podría integrar información de otras fuentes para enriquecer el análisis y mejorar la detección de fraude.