

# Sistema de Detección de Fraude con Tarjetas de Crédito usando Machine Learning

Diplomatura en Ciencia de Datos y Análisis Avanzado

**Autores:** Arenas, Diego; Díaz, Augusto; Galermes, Joaquín; Palazón, Agustina; Telis, Mónica; Vidable, Ignacio

**Fecha:** Octubre 2025





# Resumen Ejecutivo

## Problema Crítico

El fraude con tarjetas de crédito representa pérdidas millonarias anuales y erosiona sistemáticamente la confianza de los usuarios en los sistemas financieros modernos.

## Solución Implementada

Desarrollamos un sistema avanzado de Machine Learning que detecta fraudes con un recall del 88% y AUC-PR de 0.878, optimizando la precisión predictiva.

## Impacto Esperado

Reducción significativa de pérdidas económicas, mejora de la eficiencia operativa y fortalecimiento de la confianza de los clientes en el ecosistema financiero.





# Definición del Problema

## Escasez de Fraudes

Menos del 0,2% de las transacciones son fraudulentas, creando un desafío de desbalance extremo en los datos que requiere técnicas especializadas de tratamiento.

## Desafío Técnico

Necesidad de alta precisión en la detección sin generar exceso de falsos positivos que afecten la experiencia del usuario legítimo.

## Objetivo Central

Desarrollar un modelo predictivo robusto y confiable que prevenga pérdidas económicas mediante la identificación temprana de patrones fraudulentos.

# Relevancia Estratégica para el Negocio



## Impacto Financiero Global

Las pérdidas anuales por fraude con tarjetas de crédito alcanzan miles de millones de dólares a nivel mundial, representando un costo operativo crítico para la industria financiera.

## Prioridad Estratégica

La detección de fraudes constituye una prioridad estratégica fundamental para bancos, fintechs y procesadores de pagos en el ecosistema financiero actual.

## Enfoque Operativo

La estrategia óptima consiste en minimizar los fraudes no detectados (falsos negativos) aceptando un nivel controlado de falsos positivos para maximizar la protección.





# Conjunto de Datos Utilizado

284.807

Transacciones

Registros totales analizados del dataset europeo de 2013 obtenido de Kaggle

31

Variables

28 componentes PCA + Amount + Time + Class para análisis integral

0,17%

Fraudes

Porcentaje de transacciones fraudulentas en el dataset

El principal desafío identificado fue el **fuerte desbalance de clases**, requiriendo técnicas especializadas de balanceo para optimizar el rendimiento del modelo predictivo.

# Análisis Exploratorio de Datos (EDA)



## Patrones de Montos

Los montos bajos predominan en las transacciones, con los fraudes mostrando distribuciones específicas que permiten identificar patrones distintivos de comportamiento.



## Temporalidad

Los fraudes son significativamente más frecuentes durante las horas de madrugada, revelando patrones temporales críticos para la detección.



## Valores Atípicos

Se identificaron 31.904 outliers (~11% del dataset) que requieren tratamiento especializado para no comprometer la calidad del modelo.

El dataset presenta **alta calidad** sin valores faltantes, facilitando el procesamiento y análisis posterior.







# Preparación de Datos y Metodología

01

---

## Limpieza de Datos

Identificación y tratamiento de valores atípicos, normalización de formatos y validación de integridad de los datos.

02

---

## Escalado de Variables

Aplicación de técnicas de normalización para homogeneizar las escalas de las variables y optimizar el rendimiento de los algoritmos.

03

---

## Balanceo de Clases

Implementación de SMOTE y técnicas de undersampling para abordar el desbalance extremo entre transacciones legítimas y fraudulentas.

04

---

## Ingeniería de Features

Creación de la variable "Hour" a partir del timestamp para capturar patrones temporales relevantes en el comportamiento fraudulento.

**Marco Metodológico:** CRISP-DM para garantizar un enfoque estructurado y reproducible en todo el proceso de desarrollo.

# Modelos de Machine Learning Evaluados

1

## Regresión Logística

Modelo base lineal para establecer benchmark de rendimiento y interpretabilidad de resultados.

2

## Árbol de Decisión

Algoritmo interpretable que permite comprender las reglas de decisión del modelo de forma transparente.

3

## Random Forest

Ensemble de árboles que mejora la robustez y reduce el overfitting mediante agregación de múltiples predictores.

4

## XGBoost

Algoritmo de gradient boosting optimizado que demostró el mejor rendimiento en métricas críticas.

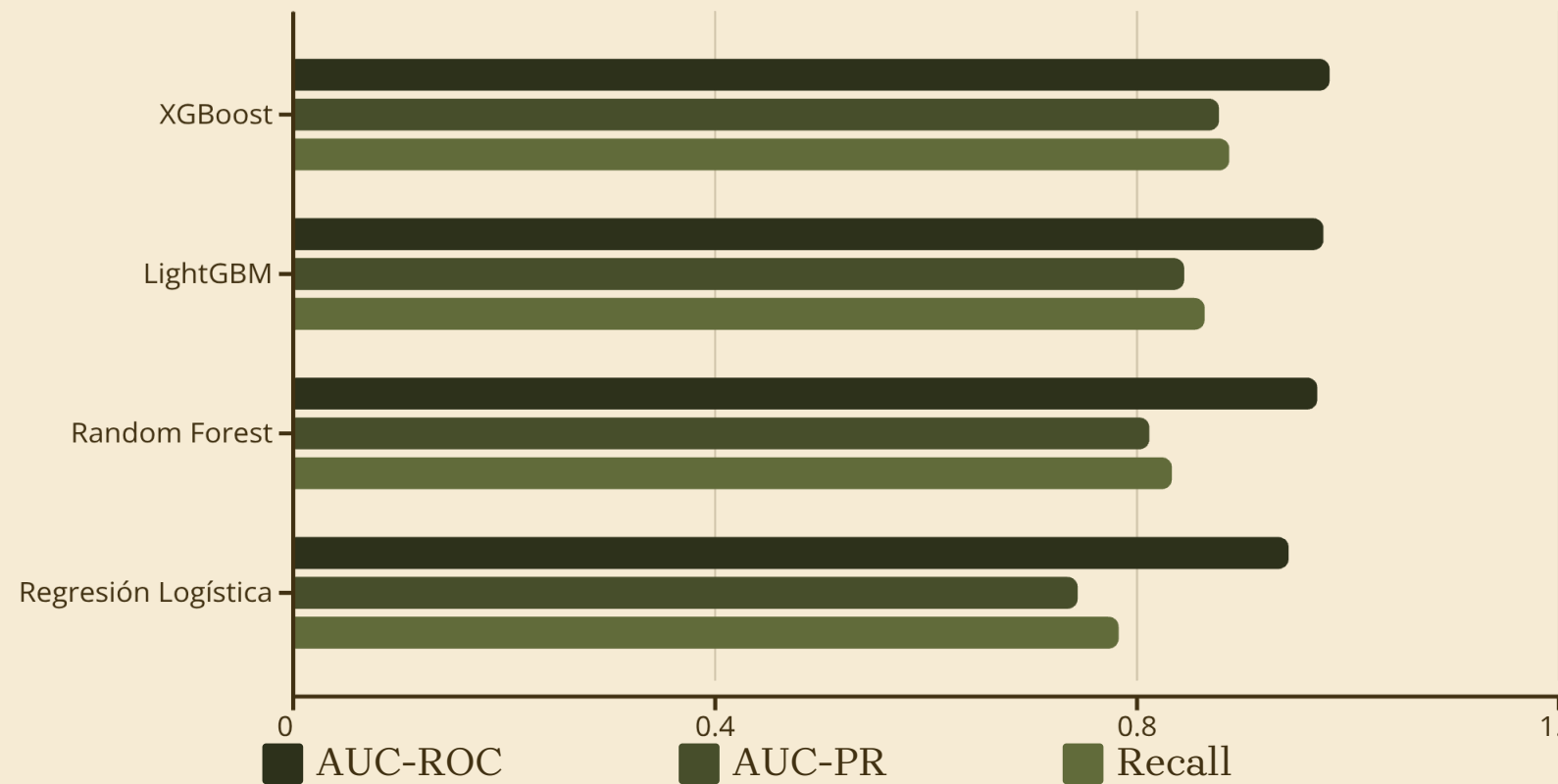
5

## LightGBM

Implementación eficiente de gradient boosting con ventajas en velocidad de entrenamiento y memoria.







# Resultados Comparativos de Modelos



**XGBoost** emergió como el modelo superior con  $\text{AUC-ROC}=0.983$ ,  $\text{AUC-PR}=0.878$  y  $\text{Recall}=0.888$ , demostrando la mejor capacidad de detección de fraudes.



# Métricas

	AUC_ROC	AUC_PR	RECALL	PRECISION	F1	TN	FP	FN	TP
 LOGISTIC REGRESSION	0.970952	0.712809	0.908163	0.055452	0.104521	55348	1516	9	89
 DECISION TREE	0.856949	0.543970	0.714286	0.760870	0.736842	56842	22	28	70
 XGBOOST	0.983255	0.877673	0.846939	0.864583	0.855670	56851	13	15	83
 RANDOM FOREST	0.967009	0.864970	0.765306	0.949367	0.847458	56860	4	23	75
LIGHTGBM	0.768613	0.004236	0.846939	0.004691	0.009330	39253	17611	15	83



# Optimización de Umbral y Valor de Negocio

Se realizó un análisis exhaustivo para determinar el umbral de clasificación óptimo del modelo de detección de fraude.

## Metodología y Costos

La optimización se basó en un **barrido de thresholds**, calculando el costo total esperado con la siguiente matriz:

- Costo de Falso Negativo (FN): 100 unidades (fraude no detectado)
- Costo de Falso Positivo (FP): 1 unidad (transacción legítima marcada como fraude)

El umbral óptimo de **0,065** minimiza el costo esperado a **1.144 unidades**, equilibrando la detección de fraude y la minimización de falsos

Métrica	Baseline (0,5)	Óptimo (0,065)
Costo Esperado	Más alto	1.144
Falsos Negativos (FN)	Mayor	11
Recall	0,834	0,888
F1-score	0,724	0,760

# Impacto Operativo Clave

<h3>Priorización de Detección</h3> <p>El umbral de 0,065 prioriza la detección de fraudes (FN), capturando ~9 de cada 10 fraudes debido al alto costo de no detectarlos (100x FP).</p>	<h3>Reducción de Pérdidas y Eficiencia</h3> <p>Permite una <b>reducción significativa de pérdidas económicas</b> y una <b>mayor eficiencia</b> al concentrar recursos en el fraude real, con falsos positivos manejables para revisión.</p>
--	---

# Próximos Pasos

<h3>Mantenimiento del Modelo</h3> <ul style="list-style-type: none"><li><b>Reentrenamiento periódico:</b> Semestralmente o cuando el rendimiento del modelo en producción (AUC-ROC, F1-score) caiga por debajo de umbrales predefinidos.</li><li><b>Monitoreo continuo de data drift:</b> Detección de cambios significativos en la distribución de los datos de entrada o etiquetas para activar reentrenamientos urgentes.</li></ul>	<h3>Implementación Técnica</h3> <ul style="list-style-type: none"><li><b>Arquitectura de APIs:</b> Desarrollo de una API RESTful de baja latencia para predicciones en tiempo real, utilizando un enfoque <i>stateless</i>.</li><li><b>Infraestructura:</b> Despliegue en contenedores (Docker) orquestados por Kubernetes para asegurar escalabilidad horizontal y alta disponibilidad.</li></ul>
<h3>Monitoreo y Alertas</h3> <ul style="list-style-type: none"><li><b>Dashboards en tiempo real:</b> Visualización de KPIs clave como costo esperado, tasa de Falsos Negativos/Positivos por umbral, y rendimiento histórico del modelo.</li><li><b>KPIs operativos:</b> Seguimiento del tiempo de respuesta de la API, tasa de éxito de llamadas, utilización de recursos (CPU, memoria).</li></ul>	<h3>Escalabilidad y Resiliencia</h3> <ul style="list-style-type: none"><li><b>Capacidad de procesamiento:</b> Diseño del sistema para autoescalado automático basado en la carga de trabajo y el volumen de transacciones procesadas.</li><li><b>Optimización de recursos:</b> Implementación de técnicas de optimización para el uso eficiente de CPU/GPU y gestión de memoria.</li></ul>