
Universidad Espíritu Santo®

**MAESTRÍA EN INTELIGENCIA DE NEGOCIOS Y CIENCIA DE DATOS**

MODALIDAD: ONLINE

# Detección de fraudes en transacciones financieras

INTELIGENCIA ARTIFICIAL


## Grupo 7

- ANA LUCIA ESPINOZA AGUILERA
- ANDREA KATHERINE ORDOÑEZ ROLDAN
- ANDREA PAOLA TAPIA NICOLALDE
- CÉSAR ALEJANDRO CABRERA VÁZQUEZ


**ING. GLADYS MARIA VILLEGAS RUGEL, MSC**

**20 DE DICIEMBRE 2025**

# INFORME TÉCNICO

## Detección de fraudes en transacciones financieras

El presente proyecto tiene como objetivo el desarrollo y evaluación de un modelo de Red Neuronal Artificial (RNA) orientado a la detección de fraudes en transacciones financieras. Para ello, se emplea un conjunto de datos sintéticos que simula operaciones reales realizadas en una fintech de pagos digitales, permitiendo analizar patrones transaccionales, temporales, geográficos y tecnológicos asociados a comportamientos fraudulentos.

## Objetivo del proyecto

Desarrollar un modelo predictivo capaz de clasificar transacciones financieras como fraudulentas o legítimas, priorizando la correcta detección de eventos fraudulentos mediante métricas como Recall, Precision y F1-Score, dada la naturaleza altamente desbalanceada del problema.

## Descripción del data set

La base de datos representa un conjunto de datos sintéticos que simula transacciones financieras realizadas en una fintech de pagos digitales.
El dataset está conformado por 200.000 registros de transacciones, asociados a aproximadamente 5.000 usuarios únicos, y contempla variables de carácter demográfico, transaccional, temporal y contextual, permitiendo un análisis integral del comportamiento de los usuarios y la detección de eventos anómalos.

# INFORME TÉCNICO

## Preparación de datos

Antes del entrenamiento del modelo se realizaron las siguientes etapas de preprocesamiento: eliminación de valores nulos e inconsistentes, codificación de variables categóricas mediante One-Hot Encoding, escalado de variables numéricas utilizando StandardScaler y partición del dataset en conjuntos de entrenamiento y prueba, manteniendo la proporción de la clase fraudulenta.

## Arquitectura

Se implementó una Red Neuronal Artificial para clasificación binaria, compuesta por capas densas ocultas con funciones de activación ReLU y tanh, y una capa de salida con activación sigmoid. La función de pérdida utilizada fue Binary Crossentropy y el entrenamiento se realizó con el optimizador Adam.

## Entrenamiento del modelo

Durante el entrenamiento del modelo de red neuronal se observa que la función de pérdida (loss) disminuye progresivamente desde 0.27 hasta aproximadamente 0.003, lo que indica que el modelo logra aprender los patrones presentes en los datos y converge de manera adecuada a lo largo de las 300 épocas de entrenamiento.

```
[   1/300] loss=0.271756
[  30/300] loss=0.058873
[  60/300] loss=0.023754
[  90/300] loss=0.013797
[ 120/300] loss=0.009540
[ 150/300] loss=0.007271
[ 180/300] loss=0.005890
[ 210/300] loss=0.004973
[ 240/300] loss=0.004325
[ 270/300] loss=0.003846
[ 300/300] loss=0.003478

--- Evaluación con Umbral = 0.5 ---
Accuracy: 0.9990
Precision: 0.0000
Recall (Sensibilidad): 0.0000
F1-Score: 0.0000
Matriz de Confusión:
 [[39960     0]
 [   40     0]]
```

# INFORME TÉCNICO

## Optimización del Umbral

Luego de optimizar el umbral de decisión, se obtuvo un valor óptimo de 0.12, lo que permitió mejorar significativamente la detección de fraudes. Con este umbral, el modelo alcanzó una accuracy de 0.9992, una precision de 0.7857, un recall de 0.275 y un F1-score de 0.4074. La matriz de confusión muestra que se identificaron correctamente 11 transacciones fraudulentas y 39,957 transacciones legítimas, mientras que 29 fraudes no fueron detectados y solo 3 transacciones legítimas fueron clasificadas erróneamente como fraude. Estos resultados evidencian que, al reducir el umbral, el modelo logra detectar aproximadamente 1 de cada 4 fraudes, manteniendo un bajo número de falsas alarmas y un alto desempeño general, lo que representa una mejora clara frente al uso de un umbral estándar.

```
--- Optimización del Umbral ---
Umbral óptimo: 0.1200
Mejores métricas:
Accuracy: 0.9992
Precision: 0.7857
Recall (Sensibilidad): 0.2750
F1-Score: 0.4074
Matriz de Confusión Óptima:
 [[39957     3]
 [   29    11]]
```

## Resultados Experimentales

Los resultados experimentales demuestran que el preprocesamiento de los datos y la optimización del umbral de clasificación influyen de manera significativa en el desempeño del modelo, especialmente en un contexto de datos altamente desbalanceados, donde es fundamental priorizar métricas como Recall, Precision y F1-Score. La comparación de arquitecturas muestra que la arquitectura Simple alcanza el mejor desempeño con un AUC de 0.998509, seguida muy de cerca por la arquitectura Medium con 0.998345 y la arquitectura Deep con 0.998005, lo que evidencia que incrementar la complejidad del modelo no aporta mejoras relevantes en la capacidad de discriminación entre transacciones fraudulentas y legítimas.

```
==============================
\Comparación de arquitecturas
==============================
              AUC_Score
Arquitectura
Simple         0.998509
Medium         0.998345
Deep           0.998005
```

# Conclusiones

En este proyecto se desarrolló un modelo de Red Neuronal Artificial para la detección de fraudes en transacciones financieras, trabajando con un conjunto de datos altamente desbalanceado. Los resultados muestran que, aunque el modelo obtiene una alta accuracy, esta métrica por sí sola no es suficiente para evaluar el desempeño en problemas de fraude, ya que con un umbral estándar no se detectan transacciones fraudulentas.

Al optimizar el umbral de decisión, se logró mejorar significativamente el recall y el F1-Score, permitiendo al modelo identificar una mayor cantidad de fraudes sin incrementar excesivamente los falsos positivos. Esto demuestra la importancia de ajustar el umbral y priorizar métricas adecuadas en este tipo de problemas.

Finalmente, la comparación entre arquitecturas indica que modelos más simples pueden ofrecer un rendimiento similar o incluso superior a modelos más complejos, lo que resalta la eficiencia del enfoque utilizado. En conclusión, el modelo desarrollado es funcional y sienta una base sólida para futuras mejoras en sistemas de detección de fraude.