# Inteligencia artificial para pagos seguros.

Julián David Triana Roa [*]

16 de mayo de 2025

## I. Introducción

Con el crecimiento del comercio electrónico y los pagos digitales, las tarjetas de crédito se han convertido en un medio de pago esencial en la economía global. Su uso ha simplificado las transacciones, permitiendo compras rápidas y seguras tanto en tiendas físicas como en línea.

Sin embargo, esta expansión también ha traído consigo un aumento significativo en los fraudes financieros. El fraude con tarjetas de crédito es un problema que afecta tanto a consumidores como a instituciones financieras, generando pérdidas millonarias cada año.

Los delincuentes emplean diversas técnicas, como el robo de datos, la clonación de tarjetas y ataques de phishing, para realizar transacciones no autorizadas. A medida que los métodos fraudulentos evolucionan, se hace imprescindible desarrollar soluciones avanzadas que permitan detectar y prevenir estos delitos de manera eficiente.

En este contexto, la inteligencia artificial se ha convertido en una herramienta clave para la detección de fraudes. Mediante algoritmos de aprendizaje automático y el análisis de patrones de comportamiento, es posible identificar transacciones sospechosas en tiempo real y reducir los riesgos asociados al uso de tarjetas de crédito.

## II. Objetivo

El objetivo de este proyecto es construir un modelo que pueda determinar si una transacción con tarjeta de crédito es fraudulenta. Con un enfoque de aprendizaje supervisado. Con visualizaciones para comprender la estructura de los datos y descubrir patrones interesantes.

[*]Universidad Escuela Colombiana de Ingeniería Julio Garavito, Ingeniería de Sistemas Bogotá, Colombia 2025

# III. Motivación Cualitativa

Según la Asociación de Banca Internacional, se estima que los fraudes electrónicos generan pérdidas superiores a 32 mil millones de dólares anuales a nivel global.

Los modelos tradicionales presentan tasas de detección inferiores al 80 %, con altos niveles de falsos positivos. Se espera que con técnicas de aprendizaje automático supervisado se supere el 95 % de precisión, manteniendo tiempos de respuesta por debajo de los 200 milisegundos.

La implementación de un sistema preventivo basado en IA podría disminuir hasta en un 40 % las pérdidas por fraude en instituciones que adopten esta tecnología.

Según la Comisión Federal de Comercio, hubo más de 100.000 denuncias de robo o fraude con tarjeta de crédito tan solo en 2023, cifra que es un 35 % más alta si se la compara con el 2021. Causando desconfianza en los usuarios ya que muchas veces tanto la entidad financiera o el portal de pagos se responzabilizan de los fraudes. Lo cuál debilita el uso de los portales de pago en linea prefiriendo acudir a medios de pago tradicionales de manera presencial lo que causa un retroceso en el mercado electrónico Por este motivo, es clave tomar medidas preventivas

Cerca de 6,9 % de las transacciones digitales en Colombia fueron sospechosas de fraude. Esta cifra, para el primer trimestre de 2024, representó un alza anual de 43,5 % en comparación al mismo período de 2023. Aproximadamente cuatro de cada diez colombianos reportaron haber sido víctimas de fraude digital, según la encuesta el Pulso del Consumidor de TransUnion.

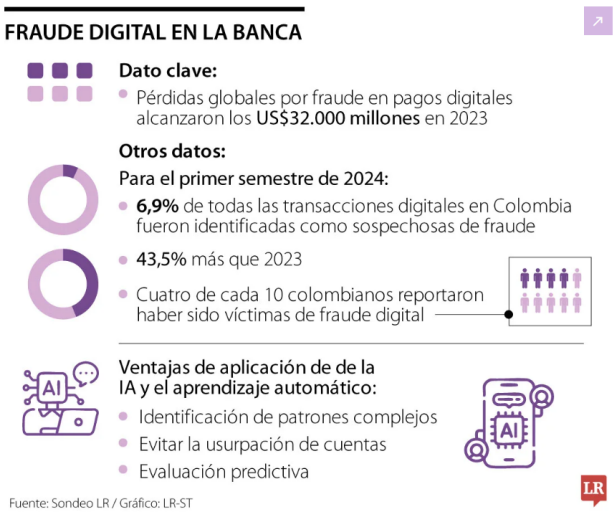



Figura 1: Datos Fraude digital en la banca

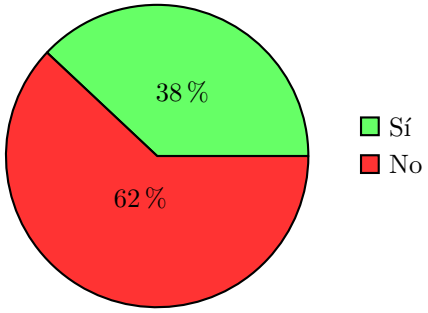
# IV. Motivación Cuantitativa

Para respaldar la investigación realizada sobre la detección de fraudes en transacciones electrónicas con tarjetas de crédito, se llevó a cabo un análisis cuantitativo basado en un conjunto de datos reales y en una encuesta aplicada a 100 personas, entre usuarios de servicios bancarios y profesionales del sector financiero. El objetivo fue obtener una visión más clara sobre el nivel de conocimiento, percepción de riesgo y confianza en las plataformas digitales de pago.

La encuesta permitió recopilar información valiosa sobre las experiencias de los usuarios respecto al fraude financiero, así como identificar puntos críticos en la relación entre los clientes y sus entidades bancarias. Este enfoque complementario fortalece la validez del proyecto, al considerar tanto el análisis técnico como el factor humano.

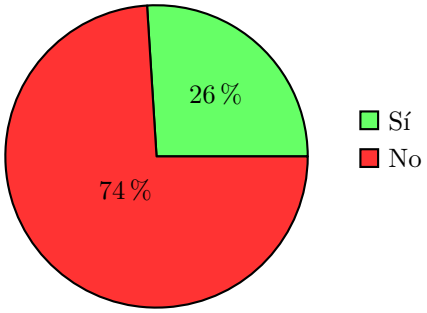
Dentro de la encuesta, se formularon varias preguntas clave para la investigación. Las más destacadas fueron:

**¿Ha sido víctima de fraude con tarjeta de crédito o débito?**



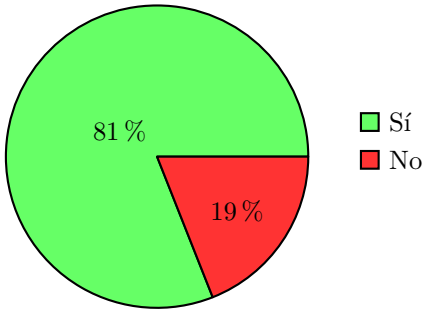

El 38 % de los encuestados respondió afirmativamente.

**¿Confía plenamente en los sistemas de seguridad de su banco?**



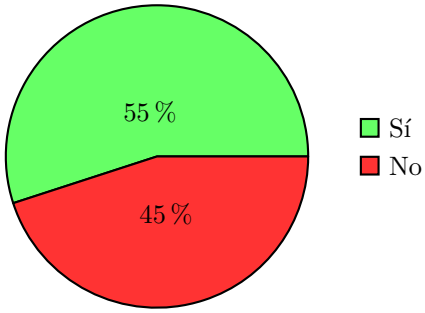

Solo el 26 % indicó tener confianza total en las medidas actuales.

**¿Cree que el uso de inteligencia artificial puede mejorar la detección de fraudes?**



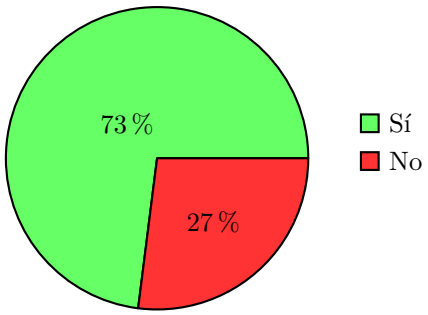

El 81 % de los participantes manifestó estar de acuerdo.

**¿Considera que el banco le informa adecuadamente sobre los riesgos de fraude?**




El 45 % opinó que la información recibida es insuficiente.

**¿Autorizaría el uso de sus datos de comportamiento para prevenir fraudes?**




El 73 % respondió que sí, siempre que se garantice la protección de su privacidad.

Estas respuestas evidencian la necesidad de implementar soluciones tecnológicas avanzadas que no solo sean eficaces en términos técnicos, sino que también generen confianza en los usuarios. A partir de los datos recopilados, se busca desarrollar un sistema predictivo que combine precisión, transparencia y protección de la información personal.

### IV.1. Problema Social

Este tipo de delito no solo impacta a los usuarios finales, sino también a las instituciones financieras, que deben asumir pérdidas millonarias y reforzar constantemente sus sistemas de seguridad. Uno de los mayores desafíos es que muchos fraudes se realizan mediante técnicas sofisticadas como phishing, robo de identidad o clonación de tarjetas, lo que dificulta su detección inmediata.

A pesar de los esfuerzos tecnológicos, los sistemas tradicionales basados en reglas fijas resultan insuficientes, ya que no se adaptan al comportamiento cambiante de los delincuentes. Como consecuencia, muchas transacciones fraudulentas pasan desapercibidas, mientras que otras legítimas son bloqueadas injustamente, afectando la experiencia del usuario.

Este entorno genera un ambiente de inseguridad y desconfianza en los canales digitales, lo cual representa un obstáculo para la inclusión financiera y la adopción de servicios en línea. Además, el incremento de fraudes también provoca una mayor carga operativa en la gestión de reclamos y en los procesos legales relacionados con delitos financieros.

## V. Resultados esperados

- **Mayor precisión en la detección de fraude** Se espera que la implementación de la solución tecnológica incremente significativamente la capacidad de las instituciones financieras para identificar transacciones fraudulentas, reduciendo el número de falsos positivos y mejorando la experiencia del usuario. .
- **Reducción de pérdidas económicas** Al identificar patrones anómalos de comportamiento financiero, la solución permitirá actuar proactivamente ante intentos de fraude, ayudando a reducir las pérdidas tanto para las instituciones como para los usuarios finales.
- **Conciencia institucional sobre inteligencia artificial** Este proyecto también contribuye a una mayor comprensión del potencial de la inteligencia artificial en el ámbito de la ciberseguridad, incentivando a las organizaciones a modernizar sus sistemas de prevención de fraude.
- **Participación activa del sector tecnológico:** El proyecto promueve la colaboración entre desarrolladores, científicos de datos y entidades financieras para crear soluciones más robustas y orientadas a problemas reales del entorno financiero actual.

# VI. Estado del arte

Para abordar la creciente problemática global relacionada con el fraude en transacciones financieras digitales, se llevó a cabo una investigación que implicó el análisis de estudios, artículos científicos y casos de aplicación relevantes en el ámbito internacional. El objetivo principal de esta investigación fue identificar las prácticas, metodologías y soluciones tecnológicas que han sido implementadas exitosamente en otros países para prevenir actividades fraudulentas en entornos bancarios y plataformas de pago en línea.

El análisis de estas fuentes proporcionó una visión detallada y multidisciplinaria de las estrategias adoptadas por instituciones financieras y empresas tecnológicas para detectar patrones de comportamiento anómalos, proteger a los usuarios y garantizar la integridad de las operaciones electrónicas. Asimismo, permitió reconocer las herramientas y modelos de inteligencia artificial más utilizados en este campo, como los algoritmos de clasificación supervisada, la detección de anomalías y los sistemas de puntuación de riesgo basados en machine learning.

Al explorar experiencias internacionales y avances tecnológicos recientes en materia de ciberseguridad financiera, se buscó extraer aprendizajes clave que sirvan de fundamento para el diseño e implementación de una solución eficaz, escalable y adaptada a las necesidades específicas de nuestro entorno local.

# VII. Arquitectura

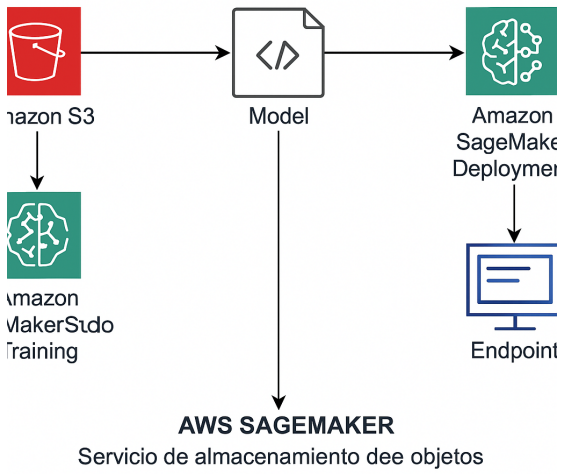



Figura 2: Arquitectura de solución AWS

Para la implementación del modelo de detección de transacciones fraudulentas, se utilizó Amazon SageMaker Studio como entorno de desarrollo y Amazon S3 como sistema de almacenamiento de datos. El conjunto de datos fue cargado en un bucket de S3 llamado fraude-transacciones-dataset, desde donde fue accedido directamente por un cuaderno Jupyter en SageMaker. En este entorno, se realizó el preprocesamiento de los datos, el entrenamiento del modelo de machine learning y su evaluación. Esta arquitectura permite una separación clara entre el almacenamiento y el procesamiento, aprovechando la escalabilidad y seguridad que ofrecen los servicios administrados de AWS.

# VIII. Descripción del caso de estudio

En este proyecto, se analizaron un conjunto de datos de transacciones con tarjetas de crédito realizadas durante un período de dos días, El conjunto de datos contiene 284.808 transacciones, de las cuáles 492 fueron catalogadas fraudulentas es decir el 0,17 % de las transacciones analizadas. Cada transacción tiene 30 características, todas ellas numéricas. Las características V1 a V 28 son el resultado de una transformación PCA, para poder proteger la confidencialidad por ello la información básica sobre estas funciones no está disponible. La función Tiempo contiene el tiempo transcurrido desde la primera transacción, y la función Monto contiene el monto de la transacción. La variable de respuesta Clase, es 1 en el caso de fraude y 0 en caso contrario.

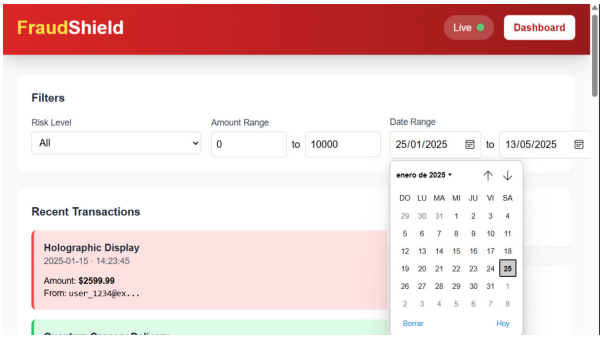
# IX. Procedimiento

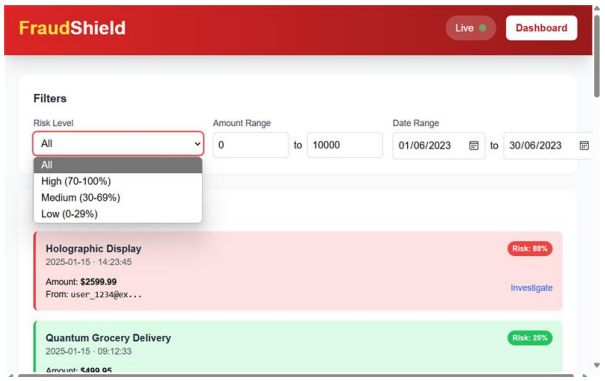
Para el procedimiento de identificación de un fraude electrónico, primero se realiza la preparación de los datos (muestreo, normalización e imputación) que luego ingresan en el modelo de aprendizaje automático, el cuál analiza los datos etiquetados que previamente fueron muestreados para su entrenamiento, segundo crea un modelo de detección basado en su aprendizaje, tercero ingresan los datos de validación, para la comprobación de sus predicciones con los que ya fueron identificados en el dataset.

# X. Experimento

En este demo, se presentará el funcionamiento básico del sistema de detección de fraudes en tarjetas de crédito, cuyo objetivo es permitir que una entidad financiera pueda analizar transacciones en tiempo real y detectar aquellas que representen un posible riesgo de fraude. La aplicación demostrará los siguientes procesos:

Una vez que el sistema recibe una transacción desde el entorno bancario, esta es evaluada automáticamente por el modelo de inteligencia artificial entrenado, el cual analiza patrones de comportamiento, montos, frecuencia y otras variables relevantes. A través de una interfaz sencilla, el usuario podrá observar la predicción del sistema, visualizar el nivel de riesgo de la transacción (bajo, medio o alto), y acceder al historial de transacciones procesadas y filtrarlas por fecha, monto o tipo de riesgo.



# XI. Conclusiones

**Reducción de Riesgos y Pérdidas Financieras** - Con la implementación de esta solución, los comercios y entidades financieras pueden disminuir el impacto económico del fraude, evitando transacciones sospechosas antes de que sean procesadas. Esto contribuye a mayor confianza y seguridad en el ecosistema financiero.

- Durante el desarrollo de este proyecto se logró identificar el modelo adecuado de aprendizaje automático para la predicción de transacciones Fraudulentas que fueron realizadas por usuarios con sus tarjetas de crédito, en esta evaluación se tomaron en cuenta los modelos de bosque aleatorio, regresión logistica, redes neuronales, obteniendo como resultado el modelo con el mayor puntaje de precisión en predecir las operaciones fraudulentas que ocurrirán en los bancos y estos podrán tomar medidas para evitar esto (Planes de contingencia)

- Reducción de Risgos y Pérdidas Financieras Con la implementación de está solución,los comercios y entidades financieras pueden disminuir el impacto economico del fraude, evitando transacciones sospechosas antes de que sean procesadas. Esto contribuye a mayor confianza y seguridad en el ecosistema financiero

- El modelo está apto para cumplir el objetivo , no obstante el modelo deberá tener una constante mejora y actualización para aumentar su precisión en las nuevas modalidades de evasión hacia el sistema.

# XII. References


[1] `https://www.larepublica.co/finanzas/fraude-de-transacciones-digitales-en-colombia-4066`

[2] `https://www.lanacion.com.ar/estados-unidos/fraudes-con-tarjeta-de-credito-mas-comunes-`

[3] Ana Umaquinga, Omar Peña, Luis Zambrano. *Machine learning: Importance, advances, techniques and applications*, 2018.

[4] Robert D, Paul Kirschner. *Computers in human behavior 1001-1013*, 2012.