

# **DETECCIÓN DE FRAUDE FINANCIERO MEDIANTE MODELOS DE APRENDIZAJE AUTOMÁTICO**

**POR:**

Pedro Pablo Saldarriaga Jaramillo  
Juan Pablo Gómez López  
Wilmer Mario Leiva Esteban

**Introducción a la Inteligencia Artificial**

**Raúl Ramos Pollan**

**Universidad de Antioquia**

**Facultad de Ingeniería**

**Medellín**

## 1. Planteamiento del problema

Las organizaciones que procesan transacciones a través de medios electrónicos tienen el riesgo de que las operaciones que transen resulten fraudulentas. Esto genera millonarias pérdidas para estas empresas, por lo que es importante un sistema de seguridad que sea capaz de detectar las operaciones de esta naturaleza. Con los datos proporcionados por Vesta Corporation en la [competición lanzada](#) por la IEEE Computational intelligence Society, se plantea el reto de predecir la probabilidad de que una transacción online sea fraudulenta.

## 2. Dataset

El dataset a utilizar proviene de una competencia de kaggle en la cual se proporcionan datos de transacciones bancarias reales del e-commerce de Vesta Corporation. El dataset está compuesto por un conjunto de archivos .csv que proporcionan la información requerida, tal como los datos de la transacción, la tarjeta, el lugar de la transacción, entre otros varios.

La información está separada en dos tipos archivos principales, *"Identity"* y *"Transaction"* los cuáles están unidos por la variable *"TransactionID"*. No todas las transacciones registradas tienen la información de identificación correspondiente.

Contamos con el archivo *sample\_submission.csv* el cuál nos muestra un pequeño ejemplo de cómo deberíamos retornar o mostrar el resultado final de nuestro reporte acerca de la veracidad de las transacciones trabajadas. Este archivo contiene la siguiente información:

- **TransactionID** - Identificador de las transacciones.
- **isFraud** - Muestra la probabilidad de que una transacción sea fraudulenta.

Los archivos de tipo *"Transaction"* se dividen en dos: *test\_transaction.csv* y *train\_transaction.csv*, uno para realizar pruebas y el otro para el entrenamiento del algoritmos, respectivamente. La información que contienen ambos es la siguiente:

- **ProductCD**: Código de Producto, el producto o servicio de cada transacción
- **card1 - card6**: Información de la tarjeta de pago, tal como tipo de tarjeta, categoría, banco, país, entre otros.
- **addr1, addr2**: Dirección de facturación por región y país.
- **P\_emaildomain**: Correo del comprador
- **R\_emaildomain**: Correo del destinatario
- **M1 - M9**: Coincidencias en la información del nombre de la tarjeta, direcciones, entre otros.
- **TransactionDT**: timedelta de una fecha y hora de referencia dada.
- **TransactionAMT**: Monto del pago de la transacción en USD
- **dist** - Distancia entre las distintas direcciones
- **C1 - C14**: Contadores, tal como cuántas direcciones se encuentran asociadas a la tarjeta de pago, etc.

- **D1-D15:** timedelta, como días entre transacciones anteriores, etc.
- **Vxxx:** Características diseñadas por Vesta, que incluyen clasificación, conteo y otras relaciones de entidad.

Los archivos de tipo “*Identity*” se dividen en dos: *test\_identity.csv* y *train\_identity.csv*, uno para realizar pruebas y el otro para el entrenamiento del algoritmos, respectivamente. La información que contienen ambos es la siguiente:

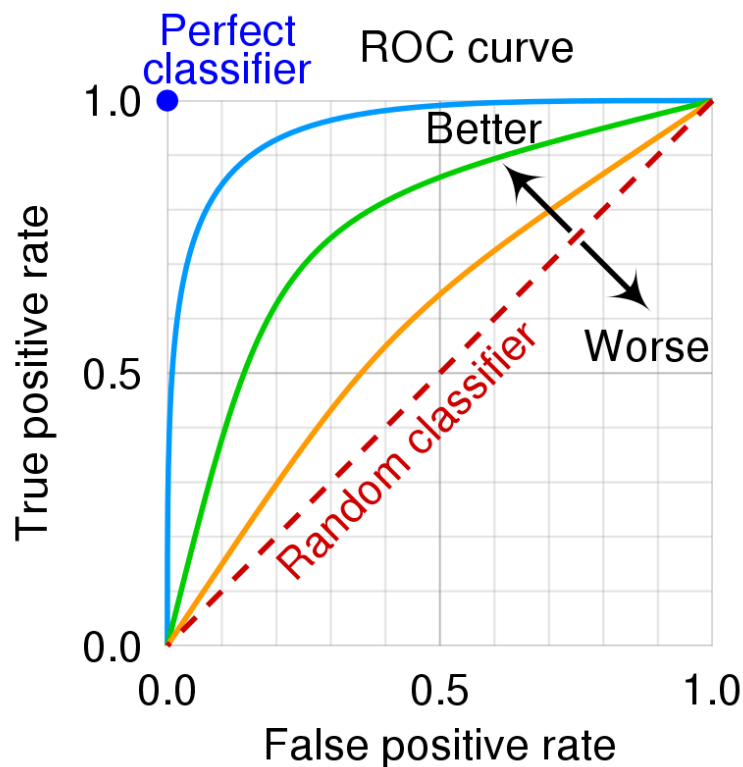
- **DeviceType:** Tipo de dispositivo en el cual se realiza la transacción
- **DeviceInfo:** Información del dispositivo en el cual se realiza la transacción
- **id\_01 - id\_38:** Características asociadas a la identidad del usuario, anonimizadas.

### 3. Métricas

La métrica de evaluación principal es la [curva ROC](#), donde se pide medir la probabilidad de que sea fraude para cada transacción. Por ejemplo, se esperan resultados de la siguiente manera:

```
TransactionID,isFraud
3663549,0.5
3663550,0.5
3663551,0.5
etc.
```

La curva AUC ROC estándar es un gráfico como el siguiente:



Obtenido de: [https://upload.wikimedia.org/wikipedia/commons/3/36/ROC\\_space-2.png](https://upload.wikimedia.org/wikipedia/commons/3/36/ROC_space-2.png)

Como métrica de negocio, la idea es disminuir lo máximo posible la cantidad de falsos positivos que el modelo arroja al analizar una transacción.

#### 4. Desempeño

La idea de colocar un modelo de esta naturaleza en producción es tal que analice de forma automática las transacciones de los clientes de X organización, y que catalogue con buena precisión las operaciones que considere como fraudulentas, y que además, el número las transacciones etiquetadas como fraude que en realidad no lo sean (falsos positivos) sea el más bajo posible.

#### 5. Bibliografía

IEEE-CIS Fraud Detection | Kaggle (2019). Retrieved March 12, 2023 from <https://www.kaggle.com/competitions/ieee-fraud-detection/>