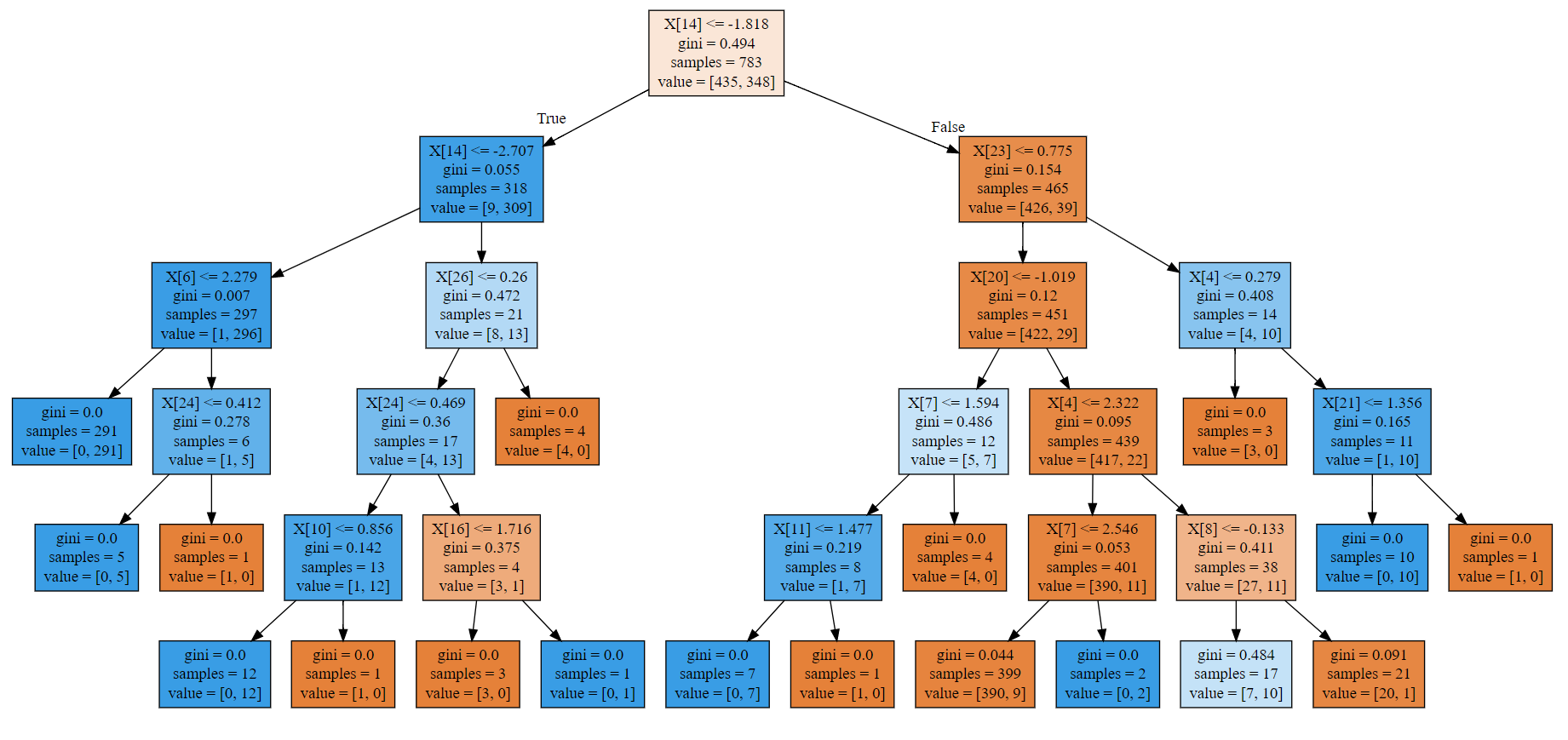
Tratamiento Inteligente de Datos

Memoria del proyecto

Detección de fraude bancario



**Grupo 4**

Javier Correa Marichal

Viren Sajju Dhanwani Dhanwani

Gabriel García Jaubert

Ángel Tornero Hernández

Índice

[1. Introducción 3](#_Toc73471208)

[2. Datos 3](#_Toc73471209)

[2.1 Descripción de los datos 3](#_Toc73471210)

# 1. Introducción

El fraude con tarjeta de crédito es una forma de estafa común cometido a través de una tarjeta de pago, ya sea de crédito o de débito. Solo en 2018, se estima que solo a través de este tipo de operaciones no autorizadas se perdió un total de 844.8 millones de libras de todo Reino Unido. Sin embargo, ese mismo año, el trabajo de bancos y de proveedores de tarjetas de créditos permitió prevenir el tráfico de 1 660 millones de libras, identificando de forma precoz la realización de actividades sospechosas y deteniendo estas operaciones. En otras palabras: de cada £3 que intentaron ser robados a través de este fraude, £2 eran detenidos con éxito por las entidades bancarias.

Puesto que este tipo de estafas se encuentra a la orden del día, se destaca la importancia de contar con un sistema que permita prevenir eficazmente este tipo de transacciones, permitiendo así evitar que los clientes afectados sean cobrados por una compra que no realizaron. En esta práctica, se plantea crear un sistema capaz de reconocer y clasificar transacciones como fraudulentas, permitiendo detener desde una etapa temprana la perpetración de este tipo de estafa.

Para ello, nuestro grupo propone dar una respuesta a través de las técnicas y algoritmos estudiados en las clases teóricas de la asignatura a las siguientes preguntas:

* ¿Podemos predecir si una transacción es o no fraudulenta? ¿Con qué grado de certeza?
* ¿Es posible encontrar un conjunto de características comunes a todas las transacciones fraudulentas?
* ¿Es viable desplegar el sistema desarrollado en un entorno real?

# 2. Datos

## 2.1 Descripción de los datos

El conjunto de datos con los que se trabajará en este proyecto fue obtenido a través del registro de las transacciones a través de tarjeta de crédito realizadas en septiembre de 2013 por compradores de origen europeo. Durante el período de 2 días, se registraron 492 operaciones fraudulentas de entre un total de 284 807 transacciones.

Puesto que estas transacciones se corresponden con operaciones de clientes reales, el conjunto de datos ha sido ofuscado con el fin de evitar revelar información personal de los afectados. Las variables que componen el dataset son el resultado de una transformación PCA, por lo que el contenido está compuesto por entrada puramente numérica. Las características del conjunto de datos han sido renombradas a través de etiquetas genéricas que ocupan el rango de ‘V1’ hasta ‘V28’; con la excepción de la columna ‘Time’ y ‘Amount’, que representan el tiempo relativo a la primera transacción grabada y la cantidad de dinero involucrada en la misma, respectivamente.

La característica ‘Class’ del conjunto de datos representa la variable de clase que se desea predecir. Esta variable categórica puede tener uno de dos valores: 0, si la transacción fue clasificada como no fraudulenta; o 1, en caso contrario. Como fue comentado brevemente con anterioridad, el número de casos etiquetados como un intento de estafa supone un 0.17% del total de transacciones registradas.

Esta característica es una de las razones que hace que este conjunto de datos sea difícil de tratar: se encuentran registradas muchas más entradas correspondientes con una variable de clase que con su contraria, por lo que mediante un entrenamiento tradicional de los modelos utilizados se podría caer en una tendencia a clasificar todas las entradas como transacciones no fraudulentas, pues esta clasificación acertaría un 99.83% de las veces. Este comportamiento no sería aceptable en un modelo donde se intenta detectar la máxima cantidad de fraudes cometidos posible, por lo que se ha de estudiar una forma de reducir la dimensionalidad de los datos del conjunto de trabajo de tal forma que se pueda obtener un resultado similar al que se obtendría utilizando el conjunto de datos original, pero sin caer en ajustar el modelo en exceso para la detección de una variable de clase concreta.

Por esta razón, a la hora de comparar los resultados obtenidos por los distintos clasificadores utilizados a lo largo de este proyecto se utiliza como métrica la exhaustividad antes que la precisión del modelo. Esto es: se desea que todos los casos fraudulentos sean etiquetados como tal, aún si ello implica etiquetar colateralmente como intento de estafa operaciones lícitas realizadas por los compradores. Se da prioridad a la minimización de los falsos negativos, afectando así al número de falsos positivos obtenidos como resultado de la clasificación.